Security and Time Management Solutions

Manual de Usuario para Equipos con Pantalla de 3 Pulgadas con Reconocimiento Facial y Huella Digital

Versión: 3.3
Fecha: Nov 2013

Acerca de este manual

Este documento introduce al uso y configuración de los equipos con pantalla de 3 pulgadas con reconocimiento facial y Huella dactilar también contiene información acerca de las diferentes configuraciones de los mismos.

Información importante

En primer lugar gracias por haber adquirido esta terminal, antes de utilizarla lea detenidamente este manual para evitar daños innecesarios. La compañía le recuerda que el buen uso del dispositivo mejorará la velocidad de autenticación.

Sin consentimiento por escrito por parte de nuestra empresa a cualquier unidad o individuo no se le permite extraer o copiar el contenido de este manual, parcial o totalmente.

El producto descrito en este manual tal vez incluye el software con los derechos de autor estos son compartidos por nuestra compañía a excepción de la autorización del titular correspondiente, cualquier persona no podrá copiar, distribuir, revisar, modificar, extraer, separar, desarmar, descifrar , hacer ingeniería inversa, arrendar, sesionar, sublicenciar el software ni otros actos de infracción de derechos de autor.

Debido a la constante renovación de productos, la empresa no puede realizar el producto real en consistencia con la información en este documento y cualquier conflicto derivado de la diferencia entre los parámetros técnicos reales y la información contenida en este documento, perdone cualquier cambio sin previo aviso.

Acerca de este manual

- No todos los equipos tienen la función marcada con★.
- La fotografía de este manual puede ser deferente a la real

Tabla de contenido

1. Instrucciones de Uso 1

1.1 Posición, postura y expresión de rostro. 1
1.2 Expresiones del rostro durante el enrolamiento 2
1.3 Posición de la huella★ 3
1.4 Usando la pantalla táctil 4
1.5 Operaciones Touch 5
1.6 Apariencia del equipo 7
1.7 Interfaz Principal 10
1.8 Modos de Verificación 12
1.8.1 Verificación de huella★ 12
1.8.2 Verificación de rostro 14
1.8.3 Verificación con contraseña 16
1.8.4 Verificación con Tarjeta ID ★ 17
1.8.5 Combinación de verificaciones★ 18

2. Menú Principal 21

3. Agregar Usuario 24

3.1 Ingrese un numero de ID. 25
3.2 Ingrese un Nombre 26
3.3 Enrole una huella★ 27
3.4 Enrolando una Contraseña 28
3.5 Enrolando una Tarjeta ID★ 29
3.6 Enrolando un rostro. 30
3.7 Ingresando un número de Grupo.★ 31
3.8 Modificar Derechos de Usuario 32

3.9 Enrolar fotografía★ 33
3.10 Configurar Acceso de Usuarios★ 34

4. Administración de Usuarios 37

4.1 Editar Usuarios 38
4.2 Borrar Usuarios 39
4.3 Consultar un Usuario 40

5. Configurar Comunicación 41

5.1 Configurar Comunicación 42
5.2 Configuración WIFI ★ 44
5.3 Salida Wiegand★ 47
5.3.1 Descripción de salida Wiegand 26-bits 47
5.3.2 descripción de salida Wiegand 34-bits 49
5.3.3 Formato Personalizado 51
5.4 Entrada Wiegand ★ 54

6. Configuración de Sistema 55

6.1 Parámetros Generales 55
6.2 Parámetros de Interfaz 56
6.3 Parámetros de Huella★ 57
6.4 Parámetros de Rostro 58
6.5 Configuración de Registros 60
6.6 Definición de Accesos Directos 61
6.7 Configuración de Acceso★ 64
6.7.1 Configuración de Zonas de Tiempo 64
6.7.2 Configurar Festivos 65
6.7.3 Configurar Zona de Tiempo de Grupo 67
6.7.4 Configurar Combinación de Apertura 69

6.7.5 Parámetros de Acceso de Control 71
6.7.6 Parámetros de Alarma de Coacción 72
6.7.7 Configuración de Anti-Pass back 73
6.8 Actualizar 74

7. Administración de Datos 75

7.1 Consulta de Registros 77
7.2 SMS★ 79
7.2.1 Crear un Mensaje corto 79
7.2.2 Ver un Mensaje Corto 83
7.3 Código de Trabajo 85
7.3.1 Agregar un Código de Trabajo 85
7.3.2 Editar y Borrar un código de Trabajo 86

8. Configuración de Fecha y hora 86

8.1 Configurar fecha y Hora 86
8.2 Configuración de Timbres★ 87
8.3 Horario de Verano (DLST)★ 89

9. Auto Prueba 91

10. Administración de USB 93

11. Información del Sistema 94

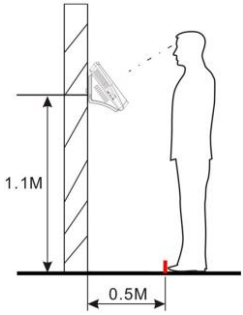
12. Apéndice 95

12.1 Instrucciones de Método de entrada T9 95
12.2 USB 97
12.3 Introducción Wiegand★ 98
12.4 Función de Foto ID★ 100
12.5 Códigos de Trabajo★ 101

12.6 Función de impresión★ 102
12.7 Modo de Verificación en Multi-Combinación★ 107
12.8 Anti-Pass Back★ 111
12.9 Declaración de Derechos Humanos y Privacidad 114
12.10 Respetuoso con el medio ambiente Uso y Descripción 115

1. Instrucciones de Uso

1.1 Posición, postura y expresión de rostro.



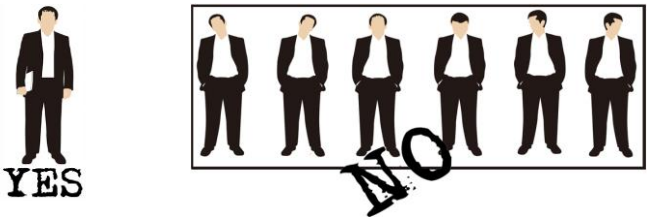
1. Distancia recomendada para la posición:

Para usuarios de 5-6 pies de altura (1.55m-1.85m) Recomendamos una distancia de 2 pies (0.5m) de la pared.

Cuando vea su imagen en la pantalla del equipo aléjese si la imagen parece muy brillante o acérquese si la imagen está demasiado oscura.

2. Recomendamos óptimas expresiones, NO extrañas expresiones:

3. Una postura normal erguida, NO posturas anormales



Nota: Durante el periodo de enrolamiento trate de relajarse para que el registro sea perfecto.

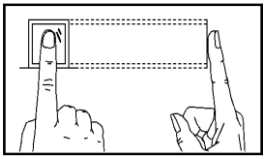
1.2 Expresiones del rostro durante el enrolamiento

Durante su registro la apariencia de su cabeza y su rostro aparecerán en la pantalla del equipo y deberá seguir los comandos de voz "Ponga los ojos dentro del cuadro verde". El usuario necesitará mover los ojos de acuerdo a la posición del cuadro verde. **Las expresiones correctas son las siguientes:**

1.3 Posición de la huella★

Dedos recomendados: dedo índice, dedo medio o dedo del anillo son los recomendados; no se recomienda el dedo gordo y el meñique.

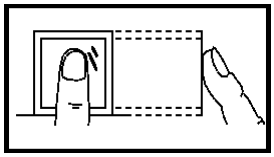
1. Posición de Huella correcta



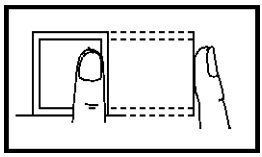
La Huella deberá estar en una posición plana total en el sensor.

2. Posición inapropiada de la huella

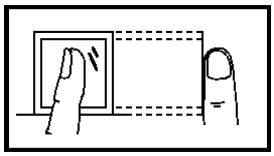
Posición no plana



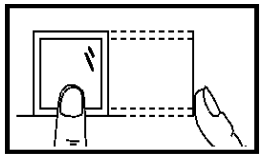
No-Centro



De lado



No-Centro



Por favor registre y verifique su huella digital utilizando el modo adecuado de colocación, no se asumirá la responsabilidad de las consecuencias que se deriven de la degradación de rendimiento de verificación debido a las operaciones inapropiadas. Nos reservamos el derecho de la interpretación final y la revisión de este documento.

1.4 Usando la pantalla táctil

Toque la pantalla con uno de los dedos o la punta de una uña como se muestra en la siguiente figura. Un punto de contacto amplio puede conducir a un error de selección.

Cuando la pantalla táctil sea menos sensible al tacto, se podrá realizar una calibración de la pantalla a través de las siguientes operaciones de menú. Presione [**Menú**] -> [**Prueba automática**] -> [**Calibración**] y la pantalla mostrará una cruz después de tocar el centro correctamente en cinco ocasiones el sistema regresará automáticamente al menú de **Auto prueba**. Presione [**Salir**] para regresar al menú principal. Para detalles, vea la descripción en 9. Prueba Automática.

La suciedad o el polvo pueden afectar al funcionamiento correcto de la pantalla táctil.

1.5 Operaciones Touch

1. Ingresar números: Presione [ID de usuario] y el sistema mostrará el teclado virtual, después de ingresar el ID del usuario solo presione [OK] para salvar o presione [X] para cancelar y regresar.

2. Ingrese un texto: Presione [Nombre] el sistema mostrará el teclado virtual ingrese el nombre y presione [Guardar] para salvar y regresar.

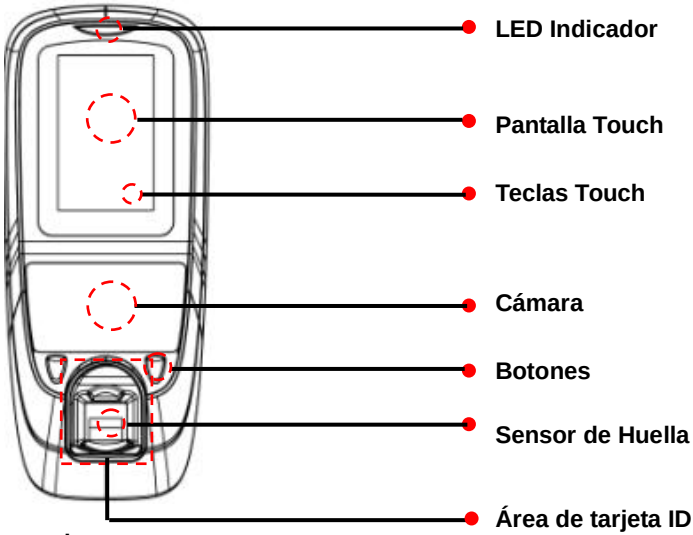
3. Modificar parámetros: Presione el valor por defecto del parámetro y el sistema cambiará automáticamente al siguiente valor de la opción escogida.

Nota: Enrolar una huella, acceso de usuario y 1: G es una función opcional que se encuentra solo en algunos equipos.

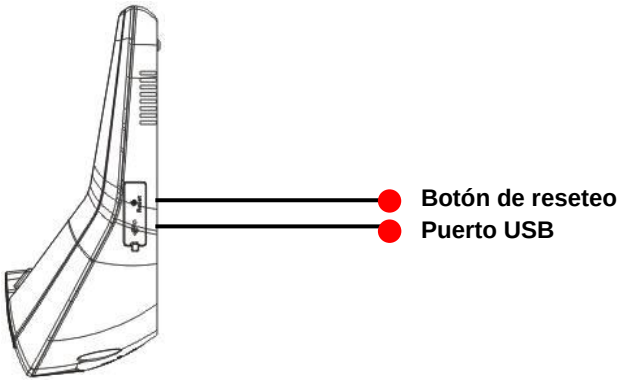
1.6 Apariencia del equipo

1. Tipo 1

(1) Vista frontal

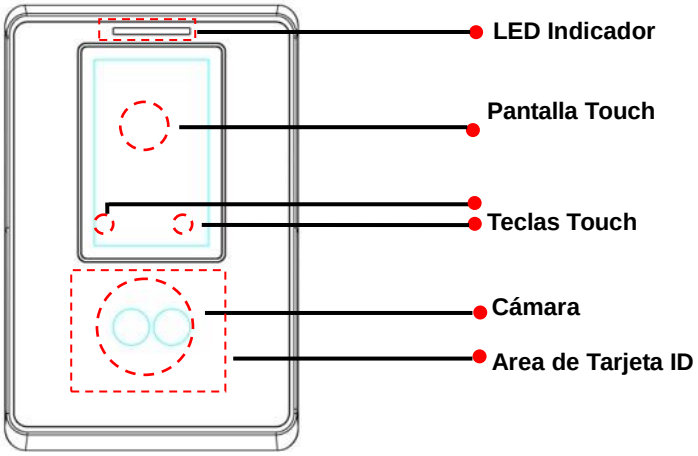


(2) Vista Lateral

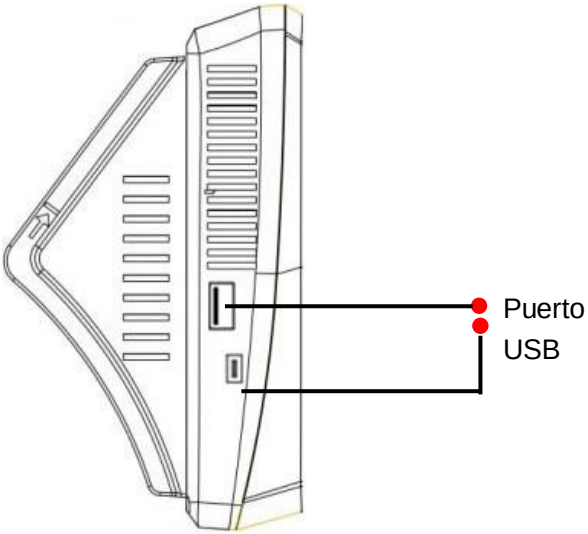


2. Tipo 2

(1) Vista Frontal

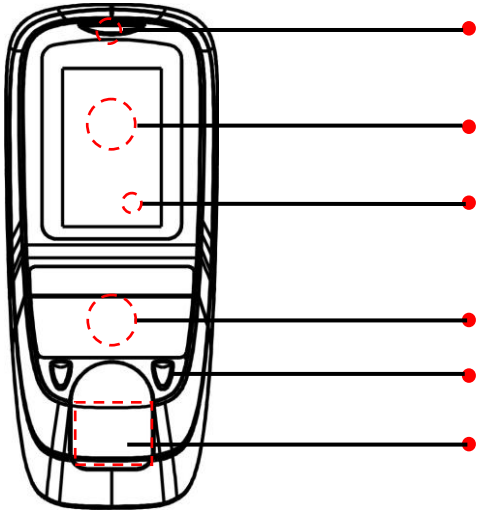


(2) Vista Lateral

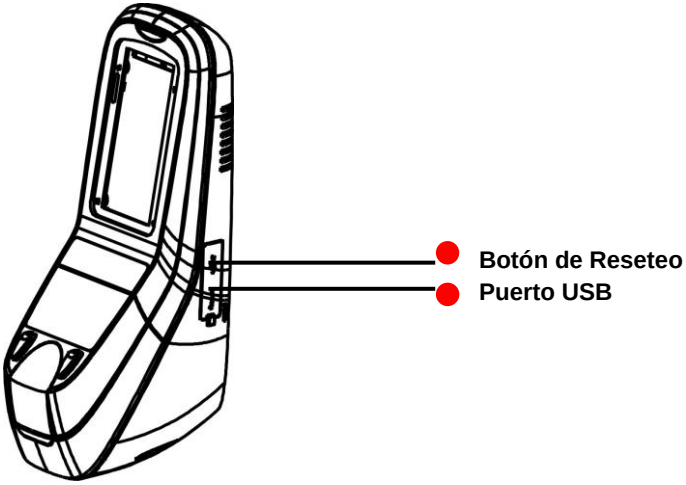


3. Tipo 3

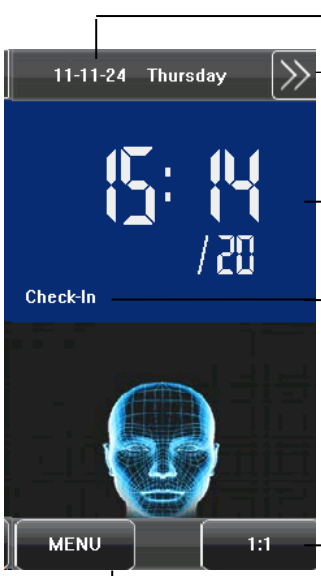
(1) Vista frontal



(2) Vista de Lado



1.7 Interfaz Principal



❖ **Fecha**

❖ **Pantalla de accesos directos**

❖ **Tiempo**

❖ **Estado de Asistencia**

❖ **Tecla de cambio a 1:1**

❖ **Menú**

① **Fecha**: Muestra la fecha actual.

② **Pantalla de teclas de acceso directo**: Muestra a las teclas de acceso directo las cuales podrán ser configurables, vea 6.6 Definir accesos directos.

③ **Tiempo**: Mostrará la hora actual, dos formatos son soportados uno de 12 horas y otro de 24.

④ **Estado de Asistencia**: Mostrará el estado actual del equipo.

⑤ **Tecla de cambio 1:1**: presionando esta tecla usted cambiará al modo de verificación 1:1 directamente desde la interfaz principal.

⑥ **Menú**: entrará al menú principal presionando esta tecla.

Nota: 1. Enrolar una huella, acceso de usuario, botón de timbre y tecla de cambio 1:1 son opcionales, solo algunos equipos las tienen.

2. El modo 1: G es opcional, si necesita esta opción por favor consulte a su oficina de ZK más cercana.

1.8 Modos de Verificación

1.8.1 Verificación de huella★

1. Verificación de Huella 1: N

La terminal compara la Huella colectada con la base de datos cargada en el equipo.

(1) Para entrar al modo de verificación el equipo automáticamente distingue de la verificación de rostro o huella solo presionando la Huella en el equipo.

(2) Presione su Huella en el sensor, para saber la posición correcta vea 1.3 Colocación de huella.

(3) si la verificación es correcta, el equipo emitirá “Verificado”.

(4) Si la verificación no es correcta, el equipo emitirá “Intente de nuevo”.

2. Verificación de Huella 1:1

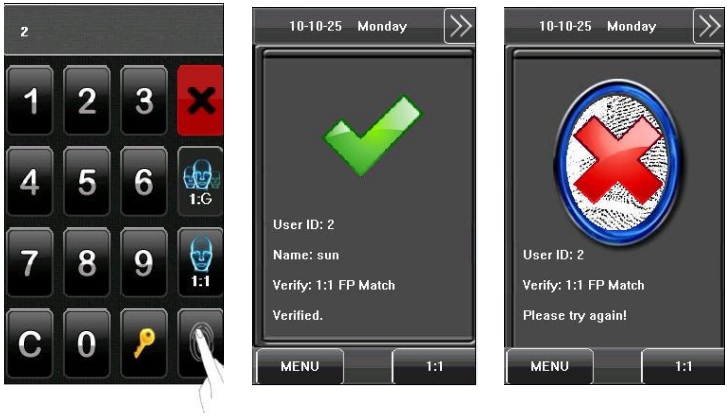
En el modo de verificación de Huella 1:1, el equipo compara la Huella actual recolectada con el modo de relación del usuario por ejemplo Numero de ID ingresado desde el teclado adopte este modo cuando la verificación sea difícil.

(1) Presione [1:1] en la pantalla o el botón [1:1] para entrar al modo de verificación.

(2) Ingrese el ID de usuario o Número de grupo después presione el icono "huella digital" para entrar al modo de reconocimiento 1:1. Si escucha "¡Usuario no registrado!" querrá decir que el ID de usuario no existe.

(3) Presione su Huella en el sensor de manera correcta. Para detalles vea 1.3 Colocación de huella

(4) si la verificación es correcta el equipo emitirá "Acceso correcto", de manera contraria emitirá "Intente de nuevo".



1.8.2 Verificación de rostro

1. Verificación de rostro 1: N ★

La terminal comparará el rostro recolectado con la base de datos.

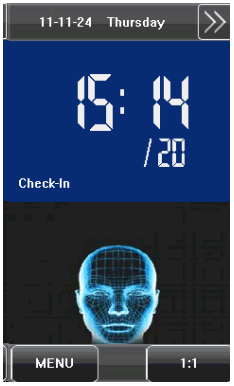
(1) El equipo automáticamente distinguirá el modo de rostro o huella.

(2) Compare que el posicionamiento del rostro sea el correcto para detalles vea 1.1 Posición, postura y expresión de rostro. La comparación se mostrará en la pantalla.

(3) Si la verificación es correcta se mostrará la fotografía de ID que fue con la que se registró al usuario.

2. Verificación de rostro 1:1

En el modo de verificación 1:1 el equipo compara el rostro colectado por la cámara y lo relaciona con ID ingresado por el teclado virtual. Se adopta este modo solo cuando es difícil el reconocimiento facial.



(1) Presione [1:1] en el botón de pantalla de inicio para entrar al modo de reconocimiento 1:1.

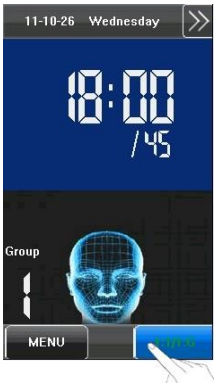
(2) Ingrese el ID de usuario después presione "1:1 rostro" es un icono para entrar al modo 1:1 si emite el comando "¡usuario no registrado!" el ID ingresado no existe.

(3) Compara que el rostro se encuentre en una manera correcta. Para detalles vea 1.1 Posición, postura y expresión del rostro.

(4) Si la verificación es correcta el equipo emitirá "acceso correcto". Y el sistema regresará a la interfaz principal pasando 20 segundos...

3. Verificación de rostro 1: G ★

Cuando abra el modo de verificación 1: G, podrá hacer la verificación 1: G. para detalles vea 6.5 Configuración de registros. El número actual del grupo, (Numero valido de grupo es 1-5) será mostrado en la interfaz de reconocimiento facial. Los usuarios en el grupo actual pueden realizar la comparación facial directamente y los usuarios de otro grupo diferente pueden realizar la comparación después de haber ingresado el Número de grupo o seleccionando y usando la tecla de acceso directo y el sistema configurará el grupo seleccionado para ser el grupo actual.

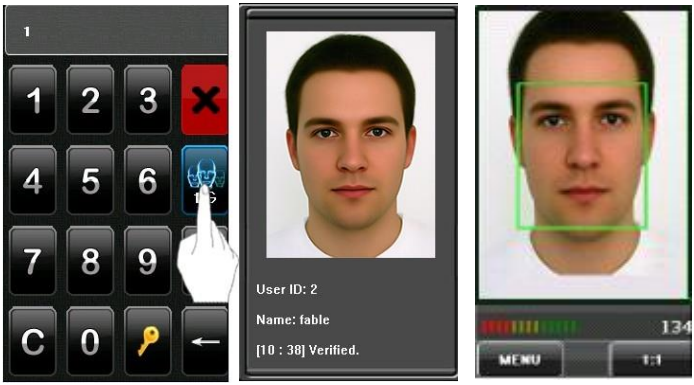


(1) Presione [1:1/1: G] para entrar al modo de verificación 1: G.

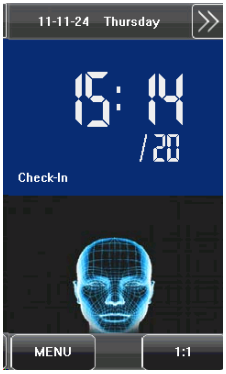
(2) Ingrese el Número de grupo y después presione "1: G" para entrar al modo de reconocimiento facial 1: G.

(3) Compare la posición del registro de rostro 1.1 Posición, postura y expresión

de rostro. El Número de grupo actual será mostrado en la figura de verificación justo como se muestra a continuación.



Nota: El modo **1: G** es una función opcional. Solo algunas terminales tienen esta opción. La función de grupo será creada solo desde la fábrica, pueden localizarla en **Sistema—Configuración de registro--1: G Verificar** y podrán usar la opción.



1.8.3 Verificación con contraseña

En el modo de verificación con contraseña el equipo tomará la contraseña ingresada y la comparará con el ID del usuario.

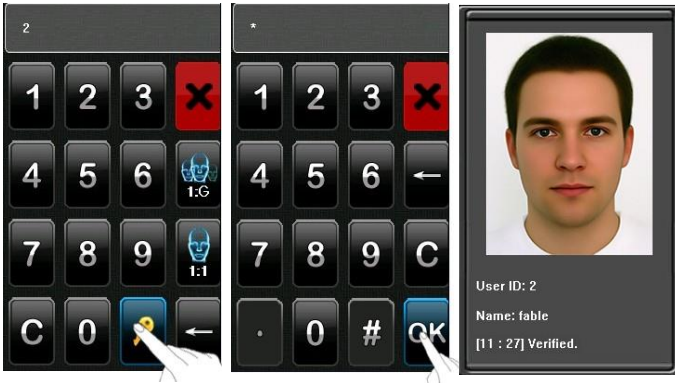
1. Presione [1:1] en la pantalla o el botón para entrar al modo de verificación de contraseña.

2. Ingrese el ID del usuario y después presione el botón en forma de llave.

3. Después ingrese la contraseña y presione “OK” para que el equipo realice la comparación.

4. Si la verificación es correcta el equipo emitirá el comando “acceso

correcto", de otra manera emitirá "verificación fallida" y regresará a la interfaz de ingreso de password.



1.8.4 Verificación con Tarjeta ID ★

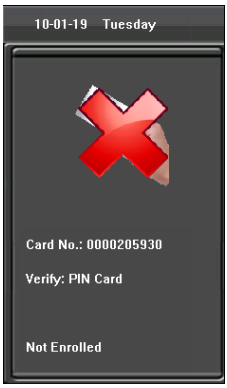
Solo los equipos construidos con un módulo de Proximidad para tarjetas ID soportan esta función. Un equipo con este módulo puede soportar las siguientes dos funciones:

Solo tarjeta ID: Solo necesitan pasar la tarjeta para una verificación con ID.

Rostro + Tarjeta ID: después de pasar la tarjeta ID será necesario también realizar una verificación facial.

1. Solo tarjeta ID

1) Pase su tarjeta ID de la manera correcta por el área designada, para información vea 1.6 Apariencia del dispositivo.
2) Si la verificación es correcta el equipo emitirá el comando "acceso correcto".
3) Si falla la verificación emitirá el comando "no registrado".



Nota:

(1) Los equipos que cuenten con la función de Foto ID se mostrará justo como en la imagen 1 de arriba;

(2) Los equipos que no cuenten con la función de Foto ID se mostrará como en la figura 2 de la parte de arriba.

2. Tarjeta ID + Verificación facial

(1) Pase su tarjeta ID por el área correspondiente para entrar al modo de verificación facial 1:1.

(2) Coloque el rostro para la verificación de una manera correcta.

(3) Si la verificación es correcta en la ventana del equipo se mostrará la verificación así como la fotografía registrada.

1.8.5 Combinación de verificaciones★

El equipo soporta arroba de 20 modos de verificación incluyendo ROSTRO&PIN/FP/RF/PW, FP&PW, FP&RF, ROSTRO&FP, ROSTRO&PW, ROSTRO&RF, FP, PW, RF, ROSTRO&PIN, FP/RF, PW/RF, FP/PW, PW&RF,

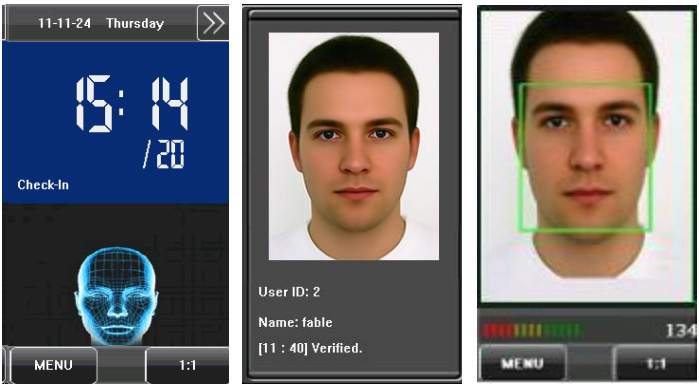
PIN&FP, FP&PW&RF, PIN&FP&PW, FP&RF/PIN, ROSTRO&FP&RF, ROSTRO&FP&PW etc.

Nota: RF significa tarjeta ID. Solo los equipos con un módulo de Proximidad instalado soportan este modo de verificación.

Aquí se muestra la combinación de modos de verificación; usaremos Rostro y Huella por ejemplo.

Si usted coloca la Huella primero y después el rostro las Operaciones serán las siguientes.

1. La interfaz principal por default es la huella vea la figura abajo.
2. Presione la Huella en el sensor de una manera correcta.
3. Si la verificación es correcta el equipo entrará al modo de verificación facial 1:1.
4. Si la verificación es correcta el equipo emitirá el comando “Verificado”. Y regresara a la interfaz principal después de 20 segundos.


11-11-24 Thursday
15: 14
/20
Check-In
MENU
1:1
User ID: 2
Name: fable
[11 : 40] Verified.
MENU
1:1

2. Menú Principal

Existen dos tipos de privilegios o derechos para otorgar a los usuarios: el **USUARIO ORDINARIO** y el **ADMINISTRADOR**. El ordinario solo tendrá el derecho para verificar con rostro, huella, contraseña o tarjeta ID en cambio el administrador tendrá el acceso al menú para modificar cada configuración del equipo e información de los usuarios.

Presione [**Menú**] para ingresar al menú principal:

Este menú incluye 9 sub menús:

Agregar usuarios: desde este submenú usted podrá agregar a un usuario incluyendo su Número de ID★, nombre y huella★, rostro, tarjeta★, contraseña, derechos, Numero de grupo. ★ Y el acceso de los usuarios★.

Administración de usuarios: Desde este submenú podrá administrar la información de los usuarios, incluyendo Numero de ID, nombre, huella★, rostro, tarjeta★, contraseña, derechos, No grupo★. Y acceso de usuario★. Aquí también podrá agregar, modificar o borrar la información deseada.

Comunicación: Desde este submenú podrá configurar los parámetros usados en la comunicación del equipo y la PC, Incluyendo dirección IP, Gateway, máscara de red, rato de baudios★, número de equipo y contraseña de comunicación.

Sistema: Configuración de parámetros básicos del sistema, parámetros de interfaz, huella★, rostro y asistencia, definición de teclado, configuración de acceso★, actualizar firmware etc.

Administración de datos: Administrará toda aquella información almacenada en el equipo por ejemplo, borrar registros de asistencia, todos los datos, borrar administradores, restablecer valores de fábrica y consultas de reportes.

Date/Time (tiempo y fecha): Configurará el tiempo y duración de alarma y de timbre.

Prueba automática: Este submenú le permitirá realizar pruebas a cada uno de los componentes del equipo para revisar su funcionamiento correcto, incluyendo pantalla, sensor, voz, rostro, teclado, reloj y calibración de pantalla.

Cargar/Descargar: Desde este submenú usted podrá descargar información del usuario y datos de asistencia almacenados en el dispositivo mediante una USB y subirla al software relacionado o a otro dispositivo de reconocimiento de huella digital.

Información del sistema: Le mostrará la información del equipo y la Capacidad del mismo con respecto a las transacciones.

Cualquier usuario podrá ingresar al menú y modificar la información del equipo SI NO SE HA CREADO UN ADIMISTRADOR una vez ya creado un administrador el equipo solo permitirá la entrada del mismo a las opciones del menú principal, recuerde que únicamente los administradores tendrán el ingreso al menú en caso de perder la contraseña de administrador puede comunicarse con su oficina local de ZK para soporte.

3. Agregar Usuario

Presione agregar usuario desde el menú principal.

ID de usuario: Ingrese el Numero de ID, el dispositivo soporta 9 dígitos por defecto.

Nombre: Ingrese el nombre del usuario, un total de 12 dígitos son soportados por defecto.

Huella★: Registre la Huella digital del usuario recuerde que esta no podrá estar repetida.

Contraseña: Registre el Numero de contraseña para el usuario, un total de 8 dígitos son soportados.

Rostro: Registre el rostro de usuario.

No de grupo.★: Configure un grupo para el usuario.

Rol: configure los derechos para el **USUARIO ORDINARIO** que será por default o podrá escoger **ADMINITRADOR**. Recuerde que al usuario ordinario solo se le permitido cualquier modo de verificación y no tendrá acceso al menú principal pero el administrador tendrá el control total del equipo.

Fotografía★: Registre una fotografía del usuario la cual será mostrada en cada verificación.

Acceso de Usuario★: Configure los parámetros de acceso para la chapa.

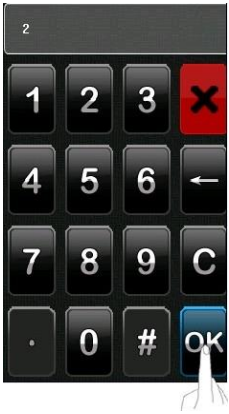
3.1 Ingrese un numero de ID

El equipo automáticamente brindará un numero de ID comenzando desde 1 y continuará en secuencia. Si usted desea usarlo de esta manera solo deberá saltar esta opción.

1. Presione [ID de usuario] y se mostrará un teclado virtual.

✍ **Tip: El Numero de ID puede ser modificado solo durante el registro una vez ya registrado el usuario no podrá ser modificado.**

2. En el teclado virtual escriba el Número deseado y después presione [OK]. Si aparece el mensaje “¡El Número de ID ya existe!” deberá colocar un nuevo número ID.



✍ **Tip: El equipo soporta como Número de ID solo de entre 1 a 9 dígitos por defecto. Si necesita extender esta opción a más Números póngase en contacto con su oficina local de ZK.**

3. Después de ingresar el Número de ID presione [Guardar] para salvar y regresar al menú anterior. Presione [Salir] para regresar sin salvar.

3.2 Ingrese un Nombre

Use el método de entrada T9 para agregar un nombre desde el teclado.

1. Presione [Nombre] desde el menú para que se muestre la interfaz.
2. Desde el teclado virtual escriba el nombre y al final presione [X].
3. Después de ingresar el nombre presione [Guardar] para salvar la información y regresar al menú anterior. Presione [Salir] para regresar al menú anterior sin salvar.

Tip: El equipo soporta de 1-12 caracteres por defecto.

3.3 Enrole una huella★

1. Presione [Huella digital] en [Agregar usuarios] para mostrar la interfaz del [Registro de huella].
2. En la interfaz mostrada, coloque el dedo en el sensor apropiadamente de acuerdo a como indica el sistema.
3. Coloque el mismo dedo en el sensor tres veces continuas. Si el registro es correcto el sistema emitirá un mensaje y regresara automáticamente a la interfaz principal. Si el registro falla mostrará un mensaje fallido y comenzará el proceso de registro.
4. Usted podrá registrar una huella de respaldo pulsando otra vez en [Huella digital]. Un usuario puede registrar hasta 10 huellas.
5. Presione [Guardar] para salvar la información y regresar a la interfaz anterior. Presione [Salir] para regresar a la interfaz anterior sin salvar la información.

3.4 Enrolando una Contraseña

1. Presione [**Contraseña**] en [Agregar usuarios] para mostrar la interfaz de administración de contraseña.
2. En la interfaz del teclado mostrada, introduzca la contraseña y presione [**OK**]. Re-introduzca la contraseña de acuerdo a lo que indica el sistema y presione [**OK**].

Tip: El equipo soporta de 1-8 dígitos por defecto.

3. después de que la contraseña es ingresada solo presione [Guardar] para salvar la información y regresar a la interfaz anterior. Presione [Salir] para regresar a la interfaz anterior sin salvar.

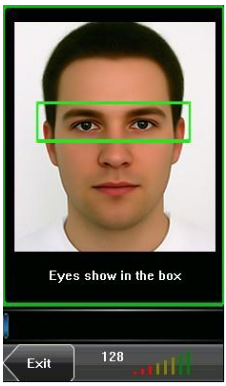
3.5 Enrolando una Tarjeta ID★

1. Presione [Tarjeta] desde el menú.
2. Se mostrará la interfaz para deslizar la tarjeta como se muestra en las imágenes de abajo, deberá pasar la tarjeta por el área del equipo especificada.
3. Si la tarjeta es pasada correctamente el equipo emitirá un comando "¡lectura correcta! No Tarjeta.: **********" y regresará a la interfaz anterior.
4. Presione [Guardar] para salvar la información y regresar a la interfaz anterior. Presione [Salir] para regresar a la interfaz anterior sin salvar

Nota: Equipos con pantalla de 3 pulgadas con reconocimiento de Huella y facial soportan la función de tarjeta MIFARE como función opcional si necesita personalizar esta función por favor contacte a su oficina local de ZK.

3.6 Enrolando un rostro

1. Presione [Rostro] desde el menú.
2. Se mostrará la interfaz de registro de rostro, mueva su cabeza de derecha a izquierda lentamente, deberá moverla de acuerdo a los comandos indicados por el equipo.
3. Si la imagen es registrada correctamente el equipo emitirá un comando y regresará automáticamente a la interfaz anterior.
4. Presione [Guardar] para salvar la información y regresar. Presione [Salir] para regresar sin salvar la información.



3.7 Ingresando un número de Grupo.★

1. Presione [No. Grupo] desde el menú

2. Observará el teclado virtual, ingrese el Número de grupo y presione [OK].

3. Después de que el número es ingresado, se mostrara la interfaz como en las imágenes de abajo, presione [Guardar] para salvar y regresar. Presione [Salir] para regresar sin salvar la información.

3.8 Modificar Derechos de Usuario

Nota: recuerde que existen solo dos tipos de usuarios **USUARIO ORDINARIO** y **ADMINITRADOR**. El usuario ordinario solo tendrá derecho a la verificación en cualquier modo, mientras que el administrador podrá modificar cada una de las configuraciones del equipo incluyendo la información de los usuarios registrados en el equipo.

1. En la interfaz [Agregar usuario], presione [Registrar usuario] para cambiarte usuario a administrador.
2. Después de terminar con la modificación la interfaz se mostrará como se muestra en las imágenes de abajo. Presione [Guardar] para salvar y regresar a la interfaz anterior o presione [Salir] para regresar a la interfaz sin salvar la información.

3.9 Enrolar fotografía★

Si usted graba una fotografía en el sistema este la mostrará junto con su ID y nombre después de que usted pase su verificación.

1. Presione [Foto] en la interfaz [Agregar usuario] para mostrar la interfaz de registro de foto.
2. En la interfaz de registro de foto, parece adquiera una posición correcta para el registro después presione [Capturar] para tomar la fotografía.
3. Después de tomar la foto presione [Salir] para regresar a la interfaz anterior.
4. Después que la foto fue tomada presione [Guardar] para salvar la información y regresar o presione [Exit] para regresar a la interfaz anterior sin salvar.

3.10 Configurar Acceso de Usuarios★

Presione [Acceso de usuario] para entrar a la interfaz de acceso de usuario.

Podrá Configurar los derechos de acceso de usuario al verificar y abrir la puerta, como el tipo de verificación, zona de tiempo, administrar la huella de coacción.

1. Tipo de Verificación

(1) Modo de verificación de grupo: Si un usuario usa este modo de verificación, deberá pertenecer al grupo.

(2) Modo de verificación Individual: Escoja el modo de verificación para el usuario, esto no afectará a los demás usuarios del grupo.

Nota:

(1) Solo los equipos con un módulo de Proximidad instalado soportarán la función de tarjeta ID.

2. Zona de Tiempo

(1) Zona de Tiempo de Grupo: El usuario usará la zona de tiempo del grupo al que pertenece.

(2) Zona de Tiempo Individual: Seleccione la zona de tiempo del usuario, esta no afectará a los demás usuarios.

3. Huella de Coacción

Puede registrar una Huella de coacción o borrar la huella que ya existe. En cualquier caso, solo si la huella de coacción registrada es verificada, se activará la alarma de coacción.

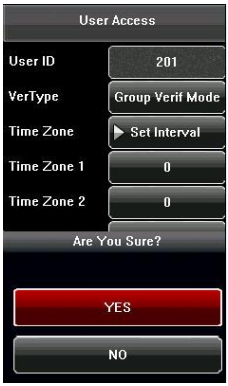
Administrar Huellas de Coacción:

(1) Registre huella de coacción

Presione [Reg. Huella de coacción] desde el menú para mostrar la interfaz de registro. Una vez dentro deberá colocar la Huella en el sensor justo como lo indica el sistema.

(2) Cancelar Huella de Coacción

Presione [Can. Huella de coacción] Desde el menú y aparecerá una ventana de confirmación. Seleccione [SI] para borrar la huella registrada, de otra manera seleccione [NO] para cancelar la operación.



4. Administración de Usuarios

Busque la información de los usuarios incluyendo ID, nombre, huella★, rostro, tarjeta ID★, contraseña, derechos, Numero de grupo.★ Y configuración de acceso de usuarios desde esta interfaz. Para agregar, editar o borrar la información básica de usuarios.

Presione [Administración de usuarios] desde el menú principal para mostrar la interfaz de administración de usuarios.

Usuarios con esta marca son administradores.

Nota: Lo usuarios se enlistan en orden alfabético por el apellido. Si presiona el nombre ingresará a la interfaz de edición del usuario para editar o borrar su información.

4.1 Editar Usuarios

Presione el nombre del usuario en la lista para entrar a la interfaz.

Solo el ID no podrá ser modificado y las demás Operaciones serán similares a agregar usuarios. Podrá re-enrolar una huella★ un rostro, cambiar la contraseña, modificar Derechos y Numero de grupo.★

Por ejemplo: Cambiar los Derechos de administrador a usuario ordinario.

4.2 Borrar Usuarios

Desde la interfaz [Información de usuario] podrá borrar parte o al usuario completo

1. Presione [Borrar] para borrar al usuario.

2. En la interfaz mostrada presione [SI] para borrarlo o presione [NO] para regresar a la interfaz anterior.

3. Desde la interfaz [Información de usuario] presione [Nombre], [huella], [rostro] o [contraseña] para borrar la información deseada y re-ingresar nueva información siguiendo los comandos del equipo.

4.3 Consultar un Usuario

Para facilitar al administrador localizar un usuario desde una larga lista de empleados, puede consultarlo directamente solo con el “ID de usuario”.

Consultar ID de usuario:

1. Presione [Consulta] en [Administración de usuarios] y aparecerá la interfaz de consulta.

2. Ingrese el Numero de ID con el teclado y presione [OK] para localizar al usuario deseado.

5. Configurar Comunicación

Usted podrá configurar los parámetros de comunicación entre el equipo y la computadora, incluyendo Dirección **IP**, **Gateway**, **mascara de red**, **rato de baudios★**, **ID de equipo**, y **clave de comunicación**.

Nota: La comunicación. (RS232/RS485), WIFI、entrada Wiegand y salida Wiegand son funciones opcionales, solo algunos equipos tienen estas funciones.

5.1 Configurar Comunicación

Dirección IP: La dirección IP es 192.168.1.201 por defecto, pero puede ser cambiada si lo requiere.

Mascara de Red: La máscara de Red es 255.255.255.0 por defecto, pero puede ser cambiada si lo requiere.

Gateway: El Gateway por defecto es 0.0.0.0 pero puede ser cambiado si lo requiere. Si el dispositivo y la computadora no están en el mismo segmento de red, necesita revisar la configuración del Gateway.

Cuando el dispositivo se comunica con la PC mediante los puertos **(RS232/RS485)★**, necesita revisar la siguiente configuración:

RS232★: Este parámetro es usado para habilitar o deshabilitar la comunicación RS232. Si son usados los cables de comunicación RS232, configure el parámetro a “ON”.

RS485★: Este parámetro usado para habilitar o deshabilitar la comunicación RS485. Si esta comunicación será usada, configure este parámetro a “ON”.

USB232★: Parámetro usado para habilitar o deshabilitar la comunicación USB232. Si esta comunicación será usada, configure este parámetro a “ON”.

Rato de Baudios★: Parámetro usado para Configurar el rato de Baudios entre la comunicación con el equipo y la PC. Incluye 5 opciones: 9600,

19200, 38400, 57600, y 115200. Es recomendado el más alto para la comunicación RS232 para una alta velocidad de archive sin en cambio un rato de Baudios más bajo es recomendado para una comunicación RS485 más estable.

ID de equipo: Utilizado para Configurar el Numero de ID del equipo de 1 a 254. Si se adopta la comunicación RS232/RS485 necesitara Configurar un Numero de ID para el equipo.

Clave de Comunicación: Para mejorar la seguridad de los datos de asistencia puede crear una contraseña de conexión entre el equipo y la PC. Una vez creada la contraseña, deberá ingresarla al conectar el equipo a la PC, de otra manera la comunicación no se podrá realizar. Por defecto es 0 (sin contraseña). Para la contraseña de 1-6 dígitos son soportados.

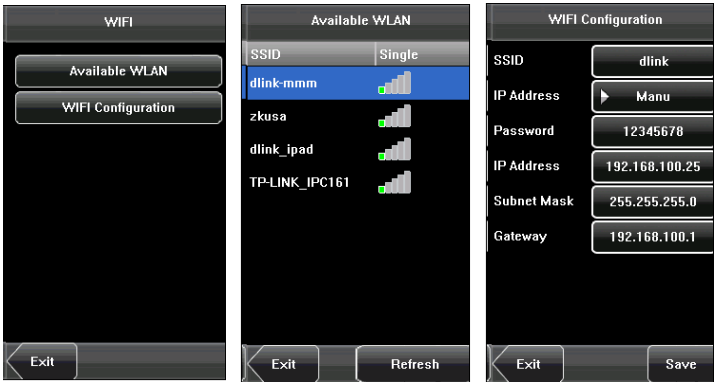
Modo de Impresión★: Cuando la verificación es correcta podrá escoger cualquier modo de impresión. El modo podrá ser configurado existen 6 modos diferentes a escoger.

Teniendo en cuenta los datos masivos incluyendo las plantillas de huellas y de rostro almacenados en el dispositivo es recomendado usar la comunicación TCP/IP como transferencia de datos entre el equipo y PC.

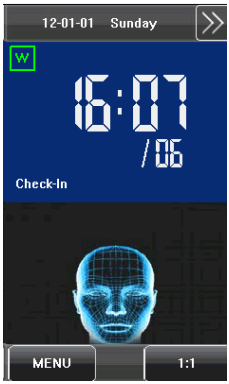
5.2 Configuración WIFI ★

1. WLANs disponibles

Se pueden buscar las señales de WLANs disponibles. Seleccione **WLAN** disponibles para entrar a la interfaz y haga clic en **Actualizar**, las señales disponibles aparecerán enlistadas en la interfaz.



Como es el tercer proceso en la figura el usuario puede escoger la señal y configurarle una contraseña. Para más configuraciones, vea "Configurar WIFI " en la siguiente sección. La contraseña deberá ser la misma del Router o modem inalámbrico exactamente como ingresaría desde su teléfono móvil con WLAN. Complete la configuración, haga clic en salvar y el equipo se conectará con el software automáticamente. La siguiente figura muestra un icono activado que indica que la conexión inalámbrica esta activa.



2. Configuración WIFI

Antes de que el equipo se conecte a la WLAN, otros componentes de la red 802.11 serán requeridos, incluyendo puntos de acceso, sistemas distribuidos y medios inalámbricos. En adición, el identificador de conjunto de servicios (ESSID) debe estar disponible.

ID de Red: Especifica la red inalámbrica a acceder. (Es sensible a letras mayúsculas o minúsculas).

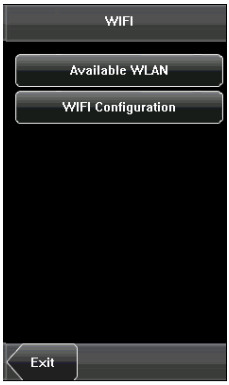
Dirección IP Local: Si la red inalámbrica 802.11 no está configurada con la función de protocolo de host dinámica (DHCP), ingrese a la interfaz manualmente e ingrese una dirección IP, mascara de red, y dirección de Gateway. De otra manera se asignará una IP dinámica.

Contraseña: Debe ser la misma del Router (Solo soporta key1 en modelos WEP.)

Dirección IP: Cuando la configuración de la dirección IP es del modo manual, asigne una dirección IP correcta, mascara de red y dirección Gateway.

Mascar de red y Gateway: Ingrese la dirección de la máscara de red y el Gateway.

Descripción de Operación



1) Configure SSID

Seleccione Configurar **WIFI** para entrar a la interfaz. Clic en el botón de ID de red e ingrese el ID de la red con el método de entrada **T9** (**IME**).

2) Configure una dirección IP local

Seleccione un modo para designar la dirección IP local. Esta será designada manualmente o en el modo DHCP.

3) Configure una Contraseña

Clic en el botón de contraseña para ingresarla usando el método de entrada **T9 IME**.

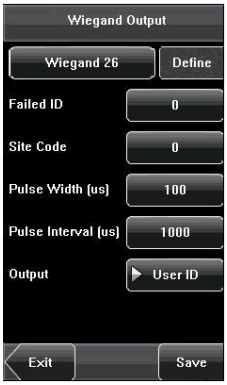
4) Asignar una Dirección IP

Configure una dirección IP valida en el dispositivo así como una máscara de red y dirección Gateway en la interfaz.

Después de asignar la dirección IP, haga clic en **Guardar** y regrese a la interfaz anterior.

5.3 Salida Wiegand★

Formato Wiegand: El sistema esta creado en dos formatos **Wiegand 26-bits** y **Wiegand 34-bits**, e incluso soportan la personalización para cualquier requerimiento.



Error de ID: Refiere al valor de salida por el sistema en una verificación fallida. El formato de salida es sujeto al "Formato **Wiegand**". El valor de alcance por defecto de **Error de ID** es 0-65535.

Código de Sitio: El código de sitios es usado para personalizar el formato Wiegand. El código de sitio es parecido al ID del equipo, pero este es personalizable y puede ser duplicado entre diferentes equipos. El valor de alcance del código de sitio por default es 0-255.

Ancho de Pulso: Se refiere al ancho del pulso Wiegand en microsegundos. El alcance del valor por default del ancho del pulso es 1-1000.

Intervalo de pulso: Se refiere al intervalo del pulso Wiegand en microsegundos. El alcance del valor por default de la anchura del pulso es 1-10000.

Salida: Se refiere a la salida del Contenido en una verificación exitosa. Puede seleccionar "ID de usuario" o "Número de tarjeta" como salida.

5.3.1 Descripción de salida Wiegand 26-bits

El sistema ha sido creado en un formato Wiegand de 26-bits. Presione [**Wiegand Format**], y seleccione "Standard Wiegand 26-bits".

La composición del formato Wiegand 26-bits contiene 2 bits de paridad y 24

bits para contenidos de salida (“ID de usuario” o “Numero de tarjeta”). El código binario de 24-bits representa arriba de 16, 777,216 (0–16, 777,215) valores diferentes.

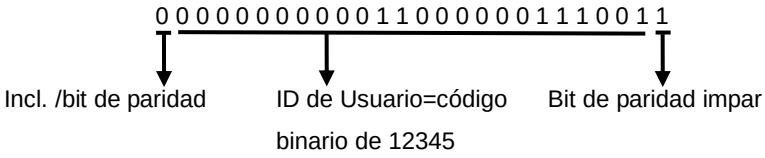
1	**2**	**25 26**
Incluso/paridad	ID usuario/Número de Tarjeta	Bit de paridad impar

Definición de Campos:

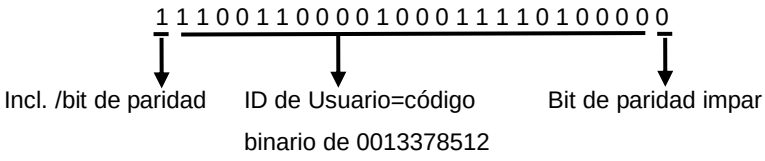
Campo	**significado**
Incluso/paridad	Juzgando del bit 2 a 13 bits. El bit de paridad par es 1 si el caracter tiene un número par de bits 1 de lo contrario, el bit de paridad par es 0.
ID usuario/Número de tarjeta (bit 2-bit 25)	ID de usuario/Número de tarjeta (Código de tarjeta, 0–16777215) El Bit 2 es el más importante Bit (MSB).
Bit de paridad impar	Juzgando del bit 14 al bit 25. El bit de paridad impar es 1 si el carácter tiene un número par de 1 bit, de lo contrario el bit de paridad impar es 0.

Por ejemplo, para un usuario con el ID de usuario 12345, el número de tarjeta inscrito es 0013378512 y el ID no se establece en 1.

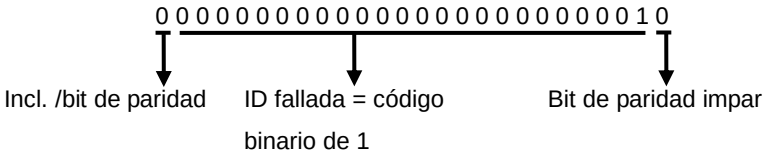
1. Cuando la salida está establecida en "ID de usuario" la salida Wiegand es la siguiente: tras la verificación exitosa:



2. cuando la salida es “Numero de tarjeta”, la salida Wiegand es la siguiente tras la verificación exitosa:



3. la salida Wiegand es la siguiente cuando la verificación falla:



5.3.2 descripción de salida Wiegand 34-bits

El sistema esta creado en un formato Wiegand 34-bits Presione [**Wiegand Format**], y seleccione “Standard Wiegand 34-bits”.

La composición del formato Wiegand 34-bits contiene 2 bits de paridad y 32 bits para salidas de contenido (“ID de usuario” o “Numero de tarjetas”). El código binario de 32-bits representa arriba de 4, 294, 967,296 (0–4, 294, 967,295) valores diferentes.

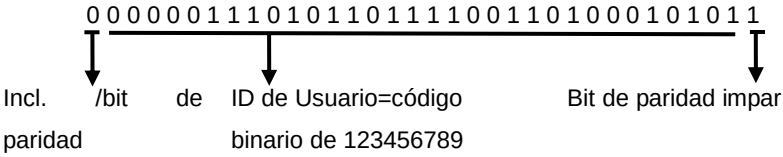
1	**2**	**33 34**
Incl./paridad Bit	ID de usuario/número de tarjeta	Paridad impar

Tabla 2 Definición de campos

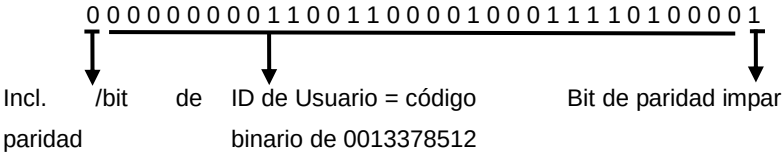
Campo	**Significado**
Incl./paridad	A juzgar desde el bit 2 al bit 17. El bit de paridad es 1 si el carácter tiene un par de bits 1. De lo contrario el bit de paridad es 0.
ID de usuario/Número de tarjeta(bit 2-bit 33)	ID de usuario/Número de tarjeta (código de tarjeta, 0–4,294,967,295) Bit 2 es el Bit más importante (MSB).
Paridad impar	A juzgar desde el bit 18 al bit 33. El **bit Impar** es 1 si el carácter tiene un número par de 1 bit; de otra manera el bit impar será 00.

Por ejemplo, para un usuario con el ID de 123456789, el Número de tarjeta enrolada es 0013378512 y el ID no se establece en 1.

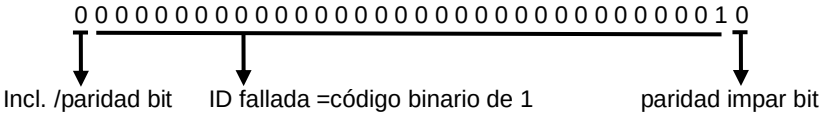
1. cuando la salida se configure a “ID de usuario”, la salida Wiegand es como se muestra a continuación:


0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1 1 1 1 0 0 1 1 0 1 0 0 0 1 0 1 0 1 1
Incl. /bit de paridad
ID de Usuario=código binario de 123456789
Bit de paridad impar

2. si la salida se ajusta a “Numero de tarjeta”, la salida Wiegand es como se muestra después de la verificación exitosa:


0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 1 1 1 1 0 1 0 0 0 0 1
Incl. /bit de paridad
ID de Usuario = código binario de 0013378512
Bit de paridad impar

3. la salida Wiegand es como se muestra después de una verificación fallida:



5.3.3 Formato Personalizado

Aparte de los dos formatos **Wiegand 26-bits** y **Wiegand 34-bits**, el sistema también soporta un formato de personalización para requerimientos individualizados.

El formato personalizado consta de dos cadenas de caracteres: el **Formato de Tarjeta** y **Formato de Paridad,** estas dos cadenas de caracteres deben ser definidas por separado.

Formato de Tarjeta: Define el Número de bits binarios de salida Wiegand así como el significado de cada bit. La salida de datos por Wiegand puede ser un Número de tarjeta (C), código de sitio (s), código de facilidad (f), código de fabricante (m) y bits de paridad (p).

Formato de Paridad bits define el modo de comparación de cada bit de datos y garantiza la exactitud de los bits de datos durante la transferencia a través de la comprobación de paridad. La paridad de bit se pueden Configurar a chequeo de impuridad (o), Inc chequeo (e) y verificación de ambos pares e impares (b). Existe una relación uno-a-uno en correspondencia entre los bits de datos y bits de paridad.

Por ejemplo, el Wiegand26 se puede personalizar como a continuación:

Definición de bits de formato de tarjeta: pssssssssccccccccccccccccp

Definición de bits de formato de paridad: eeeeeeeeeeeeeoooooooooooooo

Nota: Wiegand26 consiste de 26 bits. El primer bit es el bit de paridad del bit 2 al 13; el bit 26 es el bit de paridad impar del bit 14 al 25; del bit 2 al 9 son del código de sitio; del bit 10 al bit 25 son el Número de tarjeta.

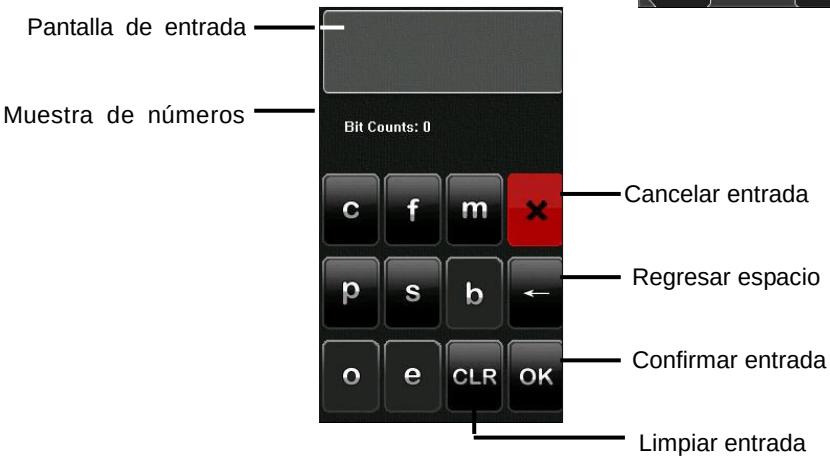
Para detalles acerca del protocolo wiegand vea INTRODUCCION DEL WEIGAND

Para personalizar el formato Wiegand, se realiza como se muestra a continuación:

(1) Seleccione [Define Format] y [Set] a continuación se habilita la tecla

(2) Presione [Set] para mostrar la interfaz [User Define Format] como se muestra en la figura:

(3) Clic en el cuadro “Card Format” para mostrar la interfaz siguiente:



Caracteres utilizados para definir el formato de los bits de tarjetas y sus significados:

C: Indica el número de la tarjeta es decir el contenido de salida que se puede configurar para ID Número de tarjeta de usuario a través de las operaciones de menú.

F: Indica el código de instalación que es 0 por defecto. No se puede configurar. Para modificarlo, por favor póngase en contacto con el proveedor del equipo.

M: Indica el código del fabricante que es 0 por defecto. No se puede configurar. Para modificarlo, por favor póngase en contacto con el proveedor del equipo.

P: Indica la posición de paridad.

S: Indica el código del sitio que se puede ajustar de 0 a 255 por defecto. **(4)** Haga clic en el cuadro de entrada debajo de "Formato de paridad" para ver la siguiente interfaz:

5.4 Entrada Wiegand ★

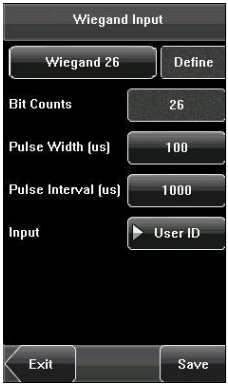
Formato Wiegand: el sistema esta creado en dos formatos **Wiegand 26-bits** y **Wiegand 34-bits**, y también soportan personalizaciones para requerimientos especiales.

Conteo Bit: Longitud de dígitos de datos Wiegand.

Ancho de Pulso: el ancho es de 100 microsegundos por defecto y se puede ajustar de 20 a 800.

Intervalo de Pulso: es de 900 microsegundos por defecto y se puede ajustar entre 200 y 20000.

Entrada: Contenido incluido en la señal de entrada Wiegand, incluyendo nombre de usuario o número de tarjeta.



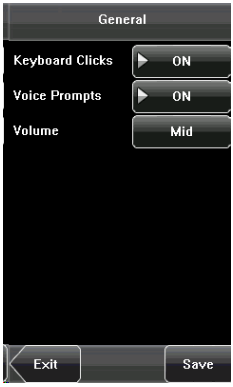
6. Configuración de Sistema

Desde el menú de Sistema podrá Configurar los parámetros del mismo, Incluyendo generales, Pantalla, Huella★, Rostro, Configuración de entrada, accesos directos, Configurar Control de Acceso★, y actualización de firmware.

6.1 Parámetros Generales

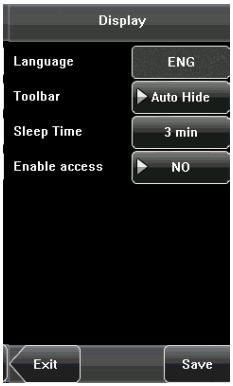
Clics de Teclado: este parámetro es usado para Configurar el sonido cada vez que presiona el teclado. Seleccione “ON” para habilitarlo o escoja “OFF” para silenciarlo.

Comandos de Voz: Este parámetro es usado para permitir los comandos de voz durante la operación del equipo. Seleccione “ON” para habilitarlos o solo “OFF” para silenciarlos.



Volumen: Parámetro usado para el ajuste del volumen durante la operación del equipo.

6.2 Parámetros de Interfaz



Lenguaje: Parámetro usado para mostrar el lenguaje usado por el equipo en equipos multi-lenguaje usted podrá escoger diferentes lenguajes. Después tendrá que reiniciar el equipo.

Barra de Herramientas: Este parámetro es usado para mostrar los accesos directos desde la interfaz principal. Se puede Configurar como “Ocultar automáticamente” y “mostrar permanentemente”. Si escoge “Ocultar automáticamente” podrá ocultarla y mostrarla manualmente. Si selecciona “mostrar permanentemente”, esta se mostrará todo el tiempo en la interfaz principal del equipo.

Hibernación (S): Este parámetro es usado como ahorro de energía para que el equipo entre al modo de reposo después de no ser usado. Usted podrá activar el equipo solo presionando cualquier tecla. El rango para este parámetro es de 1 ~ 30 minutos, por default está en 3 minutos.

6.3 Parámetros de Huella★

Umbral 1:1: Este parámetro es usado para Configurar el umbral de coincidencia de la Huella actual y la plantilla de la Huella enrolada en el equipo en el modo de verificación 1:1. Si la similitud entre la Huella actual y la plantilla de la Huella enrolada en el equipo es mayor que el umbral, la coincidencia será correcta de otra manera no será correcta.

Umbral 1: N: este parámetro es usado para configurar un umbral de coincidencia entre la Huella actual y la plantilla de la Huella registrada en el equipo en el modo de verificación 1: N. si la similitud entre la Huella actual y la plantilla enrolada en el equipo es mayor que el umbral, la coincidencia será correcta de otra manera no será correcta.

Los Umbrales Recomendados son los Siguientes:

(FRR)	(FAR)	Umbral	
		1: N	1: 1
alto	bajo	45	25
Mediano	Mediano	35	15
bajo	alto	25	10

Imagen de huella: parámetro usado para configurar cualquier modo para mostrar la imagen de la Huella en la pantalla principal, existen 4 modos a escoger:

1. **Mostar al enrolar:** Mostrará la imagen en el proceso de registro.
2. **Mostrar en comparación:** Mostrará la Huella en el proceso de verificación.
3. **Siempre mostrar:** Mostrará la Huella en el proceso de verificación y registro.
4. **Nunca Mostrar:** Nunca mostrará la imagen de la huella.

6.4 Parámetros de Rostro

Umbral 1:1: Parámetro usado para crear un umbral de coincidencia entre el rostro actual y la plantilla del rostro registrado en el modo de verificación 1:1. Si la similitud del rostro actual y la plantilla de rostro guardado en el equipo es mayor que le umbral, la coincidencia será correcta o de otra manera la coincidencia no podrá ser correcta. El alcance de valor valido es de 70-120. Cuanto mayor sea el umbral, menor será el FAR y mayor FRR y viceversa.

Umbral 1: N: Parámetro usado para Configurar el umbral de coincidencia usado entre el rostro actual y la plantilla de rostro enrolada en el equipo en el modo de verificación 1: N. Si la similitud entre el rostro actual y la plantilla enrolada en el equipo es mayor que el umbral, la coincidencia será completada o de otra manera la coincidencia no será completada. El alcance del valor valido es de 80-120.

Los umbrales recomendados son los siguientes:

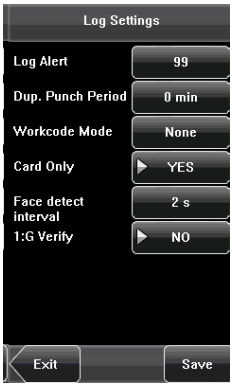
FRR	FAR	Umbral	
		1: N	1:1
alto	bajo	85	80
Mediano	Mediano	82	75
bajo	alto	80	70

Exposición: Parámetro usado para configurar el valor de la exposición de la cámara.

Calidad: Parámetro usado para Configurar la calidad del umbral para las imágenes de rostro obtenidas. El equipo acepta las imagines de rostro y los procesa mediante la adopción de un algoritmo de rostro cuando su calidad es mayor que el umbral, de lo contrario se filtran estas imágenes de rostro.

Nota: El ajuste inadecuado de exposición y de parámetros de calidad puede afectar gravemente al rendimiento del dispositivo. Por favor, ajuste el parámetro de exposición sólo bajo la supervisión del personal de servicio o post-venta de nuestra empresa.

6.5 Configuración de Registros



Registros de alerta: Cuando el espacio disponible no es suficiente para almacenar el número especificado de registros de asistencia el dispositivo generará de forma automática una alarma (valor desde: 1-99).

Periodo de registros duplicados (m): Si el registro de asistencia de un usuario que ya existe y el usuario verifica nuevamente en el plazo indicado (unidad o minutos), no se guardará el segundo registro de asistencia (Valor entre: 1-60 minutes).

Modo Código de Trabajo: Este parámetro se utiliza para seleccionar el modo de entrada de código de trabajo entre el Modo 1, Modo 2 y ninguno durante la verificación de asistencia. Si selecciona el modo 1, la verificación de la asistencia se inicia después de introducir el código de trabajo en la interfaz inicial, si se selecciona el modo 2, la verificación de la asistencia se inicia antes de ingresar el código de trabajo en la interfaz inicial; si selecciona Ninguno, deberá introducir el código de trabajo durante la verificación de la asistencia en la interfaz inicial. Para la entrada del código de trabajo, vea CODIGOS DE TRABAJO.

Solo Tarjeta★: Este parámetro si se configura en “Si”, pasará la verificación solo después de una verificación de tarjeta. Si se configure en “NO”, necesitará verificar el rostro o huellas después de verificar la tarjeta.

Intervalo de Rostro: De acuerdo a su necesidad para configurarlo. Entonces el valor por defecto es O, es decir, no tienen intervalo.

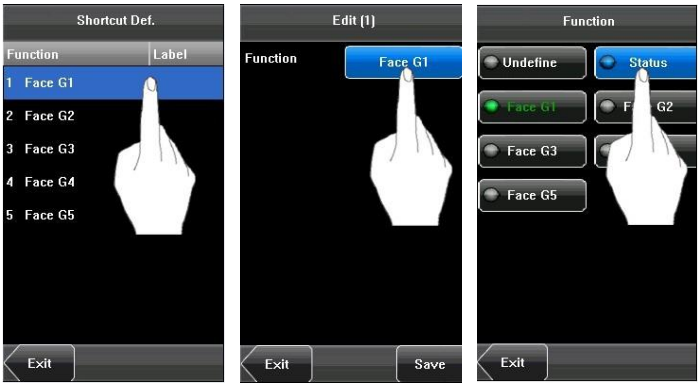
Verificación 1: G★: selecciónelo a **SI** o **NO**, se establecerá solo si se inicia esta función.

6.6 Definición de Accesos Directos

Definir teclas de acceso directo funcionales pantalla táctil. Para el dispositivo con la cara función de agrupación (MENU - Sistema - Configuración de registro - 1: G verificación), el método de definición de teclas de acceso directo se describe como sigue:

1. Configurar Teclas de Acceso Directo

Este método de acceso directo se describe de la siguiente manera:
(1) Clic en **Definir Acceso directo** para ver la lista de las teclas existentes clic en la tecla a como se ve en la figura 1. Ingrese a la pantalla de edición y haga clic en la caja **Función** como se ve en la figura 2. Dentro de esta interfaz usted podrá asignar la función deseada para cada tipo de tecla de acuerdo a sus necesidades prácticas, como 1-5 grupos de rostros (disponible para grupos de verificación), indefinido, estado, código de trabajo y SMS.



(2) El usuario puede definir una de estas teclas como una tecla de estado; clic en **Estado** como se ve en la figura 3 arriba; entre a la pantalla de edición

como se ve en la figura1 abajo; clic en **Etiqueta**, como se ve en la figura 2 abajo; entre a la pantalla de **Etiqueta**, como se ve en la figura 3 abajo; escoja la opción desea (6 opciones para estado) para realizar el cambio; el usuario puede modificar el estado de la tecla de acuerdo a la necesidad requerida.

(3) El **Código** no puede ser modificado; es cambiado de acuerdo al estado seleccionado de la tecla. Seleccione **Cambiar automáticamente,** y escoja “ON”, como se ve en la figura 1 abajo.

(4) Clic en la caja de tiempo después de “semana”, como se ve en la figura 2

arriba para entrar a la pantalla de configuración, como se ve en la figura 3 arriba. Clic en la tecla para Configurar el tiempo; clic [**OK**] para salvar y regresar a la pantalla de edición.

(5) Después de completar la configuración, haga clic en [**Guardar**] para salvar la configuración y regresar a la pantalla anterior.

2. Usando las Teclas de Acceso Directo

Clic en la interfaz principal y las teclas de acceso directo aparecerán mostrando el estado de cada una.

6.7 Configuración de Acceso★

Las opciones de control de acceso se usan para que el usuario abra la puerta en una zona de tiempo, controlando la chapa y los parámetros relacionados al equipo. No está habilitado por default de fábrica, solo deberá hacer clic en [**MENU**] - [Sistema] - [Pantalla] - [Habilitar acceso], y ahí seleccione SI o NO.

Para abrir, el usuario enrolado deberá cumplir con las siguientes condiciones:

1. La apertura actual deberá coincidir con el tiempo de la zona asignada al mismo o a su grupo perteneciente.

2. El usuario deberá pertenecer a un grupo el cual deberá tener su propia zona tiempo para realizar un verificación correcta.

Cada usuario enrolado será anexado automáticamente al grupo 1 y usará la zona de tiempo del grupo 1 y el control de acceso del grupo 1.

6.7.1 Configuración de Zonas de Tiempo

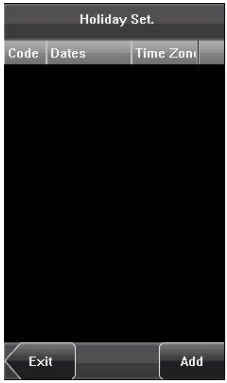
La zona de tiempo es la unidad mínima de opción de control de acceso. Se pueden definir solo 50 diferentes zonas de tiempo en el sistema Cada zona consiste de 7 diferentes secciones de tiempo (teso es una semana en total). Cada zona de tiempo es efectiva entre las 24 horas del día. Cada usuario puede pertenecer a 3 zonas. Cada sección de tiempo está en un formato **HH: MM-HH: MM**, con una precisión de minutos

Si el tiempo final es menor que el tiempo de inicio (23:57-23:56), estará prohibido el acceso todo el día. Si la hora de finalización es la hora de inicio (00:00 - 23:59), es la sección correcta. Una zona horaria efectiva para el desbloqueo de usuario es: 00:00-23:59 es más grande que la hora de inicio.

Noticia: El sistema tiene por default una sola con apertura de todo el día (esta solo podrá ser modificada no borrada).

6.7.2 Configurar Festivos

Se puede necesitar el tiempo de control de acceso especial durante los días festivos. Este es diferente a modificar, Así que el control de acceso en días festivos se puede establecer como aplicable para todos los empleados.

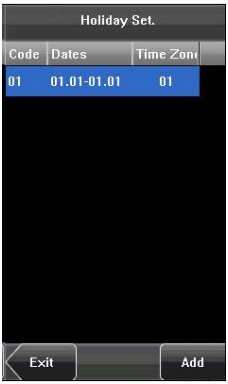


1. Agregar Festivo:

(1) Entre a la interfaz de festivo, y presione la tecla para editar los ítems.

(2) Pulse la tecla numérica de la pantalla táctil para ajustar el valor, al final presione [OK] para salvar o presione [X] para salir y regresar.

(3) Presione [Salvar] para salvar la información y regresar a la interfaz anterior o presione [Exit] para salir directamente sin salvar.



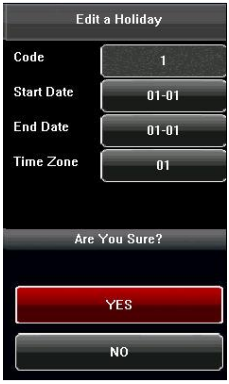
2. Editar Festivo

Seleccione el festivo a editar desde la interfaz. La operación de editar es parecida a la de agregar. Después de editar presione [Salvar] para salvar y regresar a la interfaz anterior.

Noticia: Si el tiempo de control de acceso del festivo está configurado el usuario abrirá la puerta en los días festivos solo en el tiempo establecido aquí.

3. Borrar Festivo

Seleccione el festivo a borrar. Presione **[Borrar]** y aparecerá una ventana de confirmación. Seleccione [Si] para borrar el festivo, de lo contrario [No] para cancelar la operación.



6.7.3 Configurar Zona de Tiempo de Grupo

Esta es la gestión de empleados en grupos. Los empleados de cada grupo usaran la zona de tiempo que se les asigne al grupo por defecto. Los miembros del grupo también pueden configurar la zona horaria del usuario. Cada grupo puede contener tres zonas de tiempo. El nuevo usuario inscrito pertenece al Grupo 1 de forma predeterminada y también puede destinarse a otros grupos.

1. Agregar Zonas de Tiempo a Grupos

(1) Ingrese a la interfaz de agregar y presione la tecla para editar los ítems.

Código: ingrese el Número que será el código del grupo.

Tipo de Verificación: Escoja un tipo para el grupo.

No Festivo.: selecciones la zona de tiempo será válida en el festivo

Zona de Tiempo: Seleccione la Zona de tiempo para el grupo.

(2) después de editar presione [Salvar] para salvar la información y regresar; presione [Exit] para regresar a la interfaz anterior sin salvar la información modificada.

Nota:

(1) RF significa Tarjeta ID. Solo los equipos ensamblados con un módulo de Proximidad soportan esta función.

.

Nota:

(1) Si el festivo es válido sólo cuando hay una intersección entre la zona de grupo y la zona horaria del día festivo el miembro del grupo puede abrir la puerta.

(2) Si el festivo es inválido el acceso de los usuarios no se verá afectado en lo absoluto durante el festivo.

2. Editar Zona de Tiempo de Grupo

Presione la línea a editar para ingresar a la interfaz de edición. Al terminar presione [Guardar] para salvar la información y regresar a la interfaz anterior o presione [Salir] para salir y regresar sin salvar contenido

3. Borra Zona de Tiempo de Grupo

Seleccione la línea a borrar y presione **[Borrar]**, aparecerá una ventana de confirmación, presione [Si] para borrar o presione [No] para cancelar la operación.

6.7.4 Configurar Combinación de Apertura

Hacer varios grupos en diferentes controles de acceso para lograr multi-verificación y mejorar la seguridad. Un control de acceso puede estar compuesto por 5 grupos en mayoría.

1. Agregar Combinación de Apertura

(1) Ingrese a la interfaz de agregar combinación de apertura y presione la tecla para editar los ítems.

(2) Presione en la pantalla la tecla con el Numero que desea agregar, al terminar presione [OK] para salvar y presione [X] para salir y regresar a la interfaz anterior.

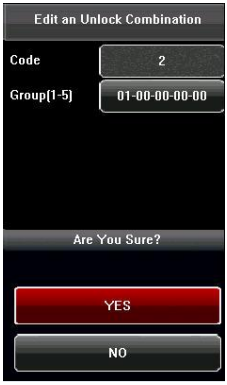
(3) Presione [Salvar] para salvar la información actual y regresar a la interfaz anterior o presione [Exit] directamente solo para regresar a la interfaz anterior sin salvar.

2. Editar Combinación de Apertura

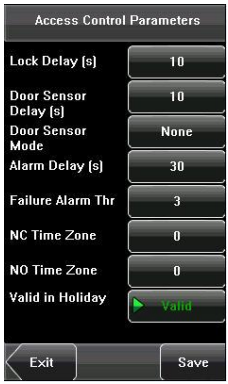
Seleccione la línea a editar Presione el ítem para entrar a la interfaz Al terminar presione [Salvar] para salvar la información actual y regresar a la interfaz anterior o presione [Salir] para regresar a la interfaz anterior sin salvar

3. Borrar Combinación de Apertura

Seleccione la línea a borrar. Presione **[Borrar]** y aparecerá la ventana de confirmación. Seleccione [SI] para borrar o escoja [No] para cancelar la operación.



6.7.5 Parámetros de Acceso de Control



Desde el menú de acceso [Access] podrá Configurar lo parámetros de las chapas magnéticas y relacionar los equipos de control de acceso.

Retardo de LOCK: Indica la duración por la que el electro imán permanecerá abierto. (Un valor de: 1-10 segundos)

Retardo de Sensor de Puerta: Indica el retardo de comprobación del sensor después de que se abrió la puerta. Si el estado del sensor de la puerta es incompatible con el estado normal establecido al sensor, se activa una alarma y este período de tiempo es considerado como "Retardo de sensor de puerta". (Un valor de: 1-99 segundos)

Modo de Sensor de Puerta: Incluye ninguno, Normalmente abierto (NO), y Normalmente cerrado (NC) "Ninguno" indica que se está usando un sensor. "NO" Indica que el estado normal de la puerta es abierto. "NC" indica que el estado normal de la puerta es cerrado.

Retardo de Alarma: Indica la duración desde la detección a la generación de señal de alarma. (Un valor de: 1-99 segundos)

Alarma de Fallo de umbral: Cuando una verificación fallida es realizada tres veces sonará una alarma (un valor de: 1-9 times).

Zona de Tiempo NC: Configure una zona de tiempo para control de acceso NC. Nadia podrá abrir la puerta durante esta zona de tiempo.

Zona de Tiempo NO: Configure una zona para control de acceso NO. el electroimán siempre estará en un estado valido durante esta zona de tiempo.

Valido en Festivo: Defina zona de tiempo para NO o NC. Cualquier que sea la zona de tiempo en festivo la zona de tiempo será válida.

Noticia:

1. Si ha sido configurado la zona de tiempo para NC o NO, cambie el sensor de la puerta a NO, De otra manera provocara una señal de alarma durante el cierre normal de la zona de tiempo o la apertura normal de la zona de tiempo.

2. Si la zona de tiempo en NC o NO, no está definida todavía, el equipo pedirá que defina una zona de tiempo y lo transferirá a la interfaz de agregar zona de tiempo.

6.7.6 Parámetros de Alarma de Coacción

Loa parámetros para Configurar una alarma de coacción. Cuando un empleado se encuentre en una situación de coacción puede Configurar la alarma de coacción como modo de verificación. El equipo abrirá la puerta como es normal pero una señal de alarma será enviada.

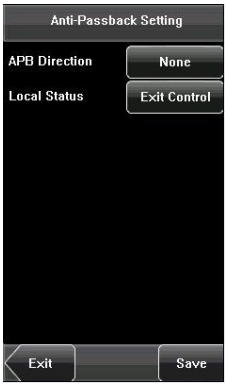
Disparador 1: 1: Si escoge “SI”, cuando el usuario use el modo 1: 1 la señal de alarma saldrá o podrá escoger por NO alarma.

Disparador 1: N: Si escoge “SI”, cuando el usuario use el modo 1: N la señal de alarma saldrá o podrá escoger por NO alarma.

Disparador de Contraseña: Si escoge “SI”, cuando el usuario use el modo de verificación de contraseña la alarma saldrá o puede escoger no a la opción.

Retardo de Alarma: Después que se inicia la alarma de coacción esta no saldrá directamente. Puede ser definido. Después del periodo de tiempo la señal de alarma será generada automáticamente (0-255 segundos).

6.7.7 Configuración de Anti-Pass back



Configurar la función de Antipassback.

Dirección APB: Existen 4 opciones: Ninguna, APB-salida, APB-entrada, APB-salida/entrada.

Estado de Equipo: existen 3 opciones: control de salida, Control de entrada y ninguno.

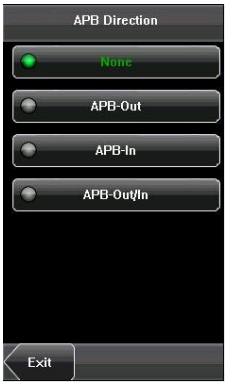
Para la función Anti-Pass back por favor vea 12.8 Anti-Pass Back.

Operación y configuración Anti-Pass back:

(1) Entre a la interfaz de Anti-Pass back y presione la tecla para editar los ítems.

(2) Presione en la pantalla la tecla para configurar el valor al terminar presione [Ok para salvar o presione [X] para salir y regresar a la interfaz anterior.

(3) Presione [Salvar] para salvar la información actual y regresar o presione [Exit] para regresar a la interfaz anterior sin salvar.



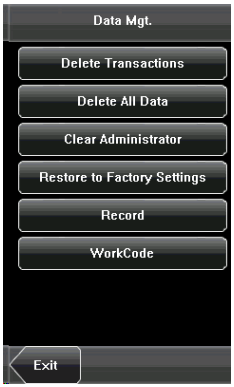
6.8 Actualizar

Puede actualizar el firmware del equipo usando un archive de actualización desde una memoria USB

Si usted necesita actualizar el firmware de su equipo póngase en contacto con su oficina local de ZK, actualmente no lo recomendamos esta opción.

7. Administración de Datos

Desde el menú [Administración de datos], usted podrá administrar todos los datos guardados en el equipo, por ejemplo, borrar registros de asistencia, borrar todos los datos, borrar administrador, restablecer a valores de fábrica y consultar registros.



Borrar transacciones: borrara todos los registros de asistencia.
Borrar todos los datos: borrar toda la información del personal registrado, incluyendo huellas, rostros y registros de asistencia.
Borrar administrador: Cambiara los administradores a usuarios ordinarios.
Restablecer a valores de fábrica: restablecerá los parámetros del equipo a valores de fábrica.

SMS★: El operador podrá crear mensajes cortos públicos o personales y mostrarlos a una persona o varias en el tiempo deseado. Como adición el operador podrá crear mensajes cortos para futuro.

Numero de Trabajo★: El operador podrá configurar uno o múltiples número de trabajo para los empleados de acurdo al tipo de trabajo de estos. Los números de trabajo pueden ser usados para calcular asistencia y salario.

☺**Noticia:** La información de empleados y su asistencia no serán borrados durante la operación de restablecimiento a valores de fábrica.

7.1 Consulta de Registros

Después de verificar entrada correctamente, el registro de asistencia del empleado será guardado en el equipo. Usted podrá fácilmente revisar esos registros.

ID de Usuario: Ingrese el ID de un usuario para una consulta. Si este campo se deja en blanco podrá consultar el registro de todos los empleados y si ingresa el ID del usuario consultara los registros de asistencia de este usuario.

Consulta de Periodo de Tiempo: Seleccione el periodo de tiempo a consultar, incluyendo un tiempo personalizado, ayer, esta semana, la semana pasada, este mes, mes pasado y todos los periodos.

Inicio y **Final**: cuando Seleccione un periodo personalizado deberá ingresar un tiempo de inicio y un tiempo final. Cuando Seleccione otras opciones para el periodo de tiempo el inicio y el final serán automáticamente relacionas al tiempo.

Después de Configurar la condiciones de consulta, presione [Consulta] y el registro especificado a las condiciones será mostrado en la pantalla.

Seleccione de la lista el registro deseado y podrá consultar a detalles la información de registro.

Por ejemplo, presione ID de usuario e ingrese a la interface, ingrese el Numero de ID y presione [Consultar], los resultados aparecerán en la pantalla.

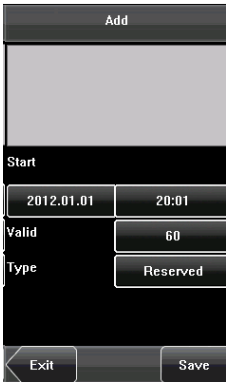
7.2 SMS★

Los mensajes cortos son similares a anuncios o noticias. Lo operadores pueden escribir un mensaje de acuerdo a las necesidades a anunciar y mostrarlo en la pantalla del equipo durante un periodo de tiempo designado. Estos serán clasificados como mensajes públicos o privados. Si se le configura como público, este será mostrado en el periodo de tiempo designado[i] y los usuarios podrán usar la teclas de acceso directo (se brinda esta opción a una o, más teclas) para ver el mensaje. Pero si el mensaje se configura como privado, solo el empleado deseado podrá visualizar esta información de mensaje.

7.2.1 Crear un Mensaje corto

1. Agregar un Mensaje Corto

a) Seleccione **Mensaje Corto** > **Agregar**:



Inicio: Significa el tiempo cuando el mensaje tomara efecto.

Valido: Significa que el mensaje será mostrado solo durante un periodo de tiempo valido.

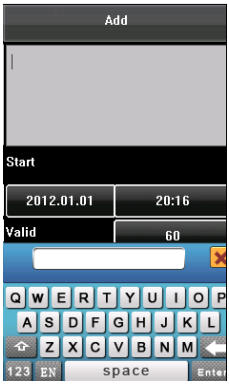
Tipo:

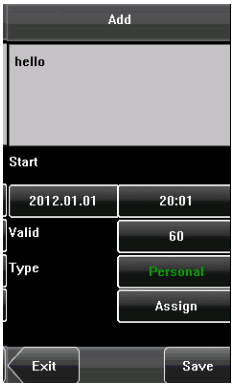
Reservado: Significa que el mensaje ha sido preparado para futuro pero no configurado como público o personal.

Personal: solo una solo persona podrá visualizar el contenido del mensaje

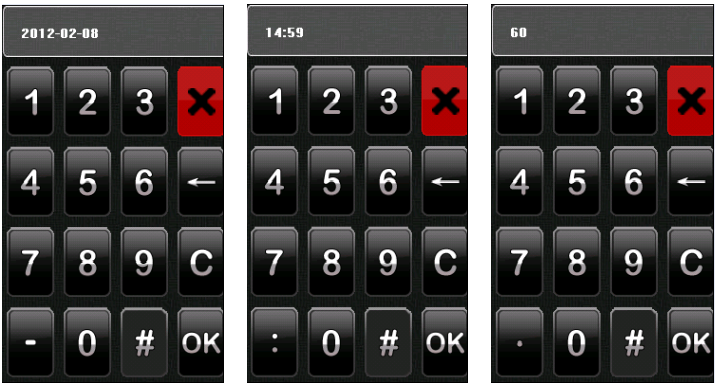
Publico: Todas las personas podrán ver el contenido del mensaje.

b) Como se ve en la siguiente figura, clic en el área de mensaje corto, usando el método de entrada **T9 IME** ingrese el contenido del mensaje.



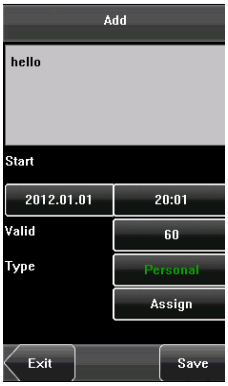


c) Clic **inicio** o **Valido** para iniciar la configuración tal y como se muestra en las siguientes figuras:

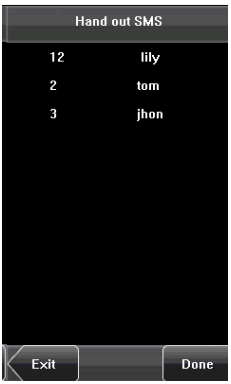


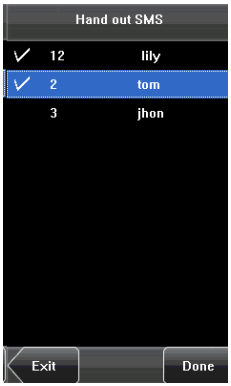
Presione el numero como el valor que será agregado y haga clic en **OK** para salvar la configuración y regresar a la interfaz.

d) Clic en **Tipo** para cambiar los tipos de mensajes, incluyendo personal, público y reservado. La siguiente figura muestra el personal:

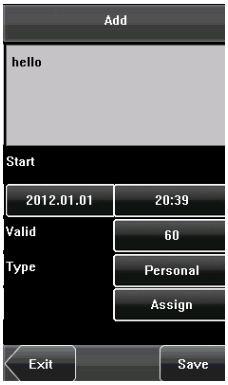


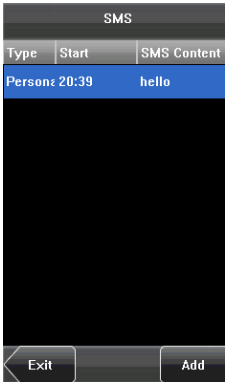
e) Clic **Repartir SMS** para entrar a la interfaz de repartición. Como se ve en la siguiente figura, haciendo clic en el nombre del empleado, este podrá visualizar el mensaje que le ha sido otorgado.





f) Como se muestra en las siguiente figuras haga clic en **Finalizar** para salvar la información regresar a la interfaz anterior. Después de eso haga clic en **Salva** para guardar el mensaje y regresar a la interfaz anterior y el mensaje será mostrado en la interfaz.

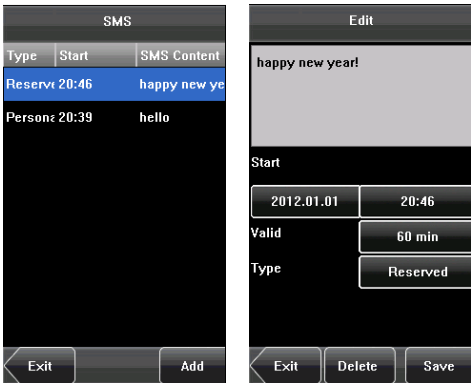




2. Editar un Mensaje Corto

Haga clic en el mensaje que será editado desde la interfaz de **SMS**.

Este procedimiento es el mismo que agregar un mensaje nuevo.



3. Borrar un Mensaje

Haga clic en **Borrar** desde la interfaz y borrara el mensaje así como la información de este.

7.2.2 Ver un Mensaje Corto

- **Ver un Mensaje Publico**

  En la interfaz principal los mensajes públicos serán mostrados automáticamente en un intervalo de minutos, los mensajes cortos pueden ser vistos usando las teclas de acceso directo localizadas al inicio, como se ve en las siguientes figuras.

Después de terminar la lectura haga clic en **Regresar** para salir de la visualización y regresar al menú principal.

- **Ver un Mensaje Personal Corto**

  Después de que el usuario verifica, su mensaje será visualizado como se ve en la siguiente figura:

7.3 Código de Trabajo

Para una distinción fácil de usuarios de otras labores u opciones haga clic **[Sistema]--[>Definición de accesos directos]--[no definido], escoja [Código de trabajo]** salvar y podrá abrir la función de código de trabajo**.**

7.3.1 Agregar un Código de Trabajo

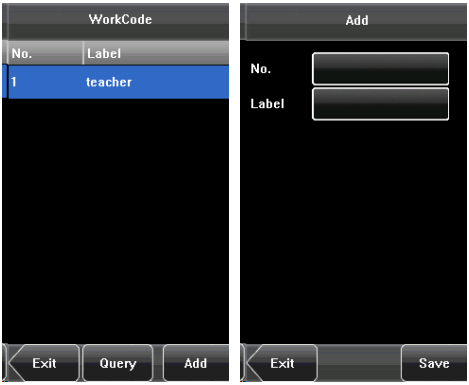
1. Presione **[Agregar]** en la interfaz para mostrar la ventana de agregar códigos de trabajo.

No.: Digito para agregar como código de trabajo.

Etiqueta: Significado de código de trabajo.

2. Presione el botón correspondiente [No.] en [Agregar] para mostrar la interfaz de agregar ya aquí ingresar un número.

3. Presione el botón correspondiente de [**Etiqueta**] en la interfaz de código de trabajo para mostrar la interfaz de entrada de texto. En este interfaz entre el código de trabajo.



7.3.2 Editar y Borrar un código de Trabajo

1. Presione sobre un código de trabajo en la lista y aparecerá la interfaz de edición [**Editar**].

2. Para editarlo ingrese un Nuevo número y etiqueta, será la misma operación y pasos de agregar un código de trabajo.

3. Para borrar el código de trabajo solo presione [**Borrar**].

4. En la interfaz emergente presione <**SI**> para confirmar el borrado de este código de trabajo o presione <**NO**> para cancelar la operación.

8. Configuración de Fecha y hora

8.1 Configurar fecha y Hora

La fecha y hora del equipo deberán ser configurados de acurdo al uso y especificación de asistencia de la empresa.

1. Presione [**Menú**] desde la pantalla principal y aparecerá el menú.

2. Presione [**Tiempo/fecha**] en este menú para entrar a la interfaz de configuración de fecha y hora.

3. Seleccione la fecha y hora deseada presionando los parámetros. Para formato de tiempo existen 10 diferentes a seleccionar. Soporta 12-horas y 24-horas como formato de hora.

4. Presione [**Guardar**] para salvar la información actual y regresar o presione [**Exit**] para regresar a la interfaz anterior sin salvar los cambios.

8.2 Configuración de Timbres★

En la mayoría de las compañías son necesitados timbres como señal de inicio o fin de un turno de trabajo y usualmente utilizan los timbres eléctricos de manera manual. Para bajar costos y maximizar la administración nosotros hemos integrado esta función al equipo. Usted podrá organizar el tiempo y duración de la alarma de acuerdo a sus necesidades por lo que el timbre será activado automáticamente a la hora configurada por usted y parara en el tiempo también especificado por usted. Cada equipo puede alojar hasta 15 tipos de timbre diferentes para que usted seleccione uno de ellos.

Presione [**Timbre**] en el menú de hora y fecha y aparecerá la interfaz de edición de timbres, como se ve en la figura de abajo.

1. Agregar Timbre

1) En la interfaz se mostrarán los timbres solo haga clic en [Agregar] para ver la interfaz de agregar.

2) en la interfaz de agregar, configure los siguientes parámetros:

Tiempo de Timbre: Parámetro usado para configurar el punto de tiempo en el que el equipo activará el timbre cada día.

Fecha de Timbre: Parámetro usado para Configurar el día en el que el equipo activara automáticamente el timbre.

Tono de Timbre: Parámetro usado para configurar tono de timbre deseado.

Volumen: Parámetro usado para configurar el volumen de sonido del timbre.

Repetir: Parámetro usado para Configurar la repetición de las timbre.

Estado: Parámetro usado para saber el estado del timbre habilitado o deshabilitado.

Tipo de timbre: Usted podrá seleccionar entre un timbre interno o externo. Para el interno este será activado por el equipo y escuchado a través del mismo. Para el externo se necesitará conectar un timbre externo al equipo.

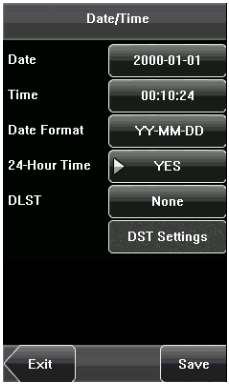
2. Editar y borrar un Timbre

Presione sobre el timbre en la lista mostrada en la interfaz clic en [**Editar**] la operación será la similar a agregar un timbre.

✍ **Noticia**: Solo algunos modelos soportan esta función. Si necesita esta función por favor contacte a su oficina local de ZK.

8.3 Horario de Verano (DLST)★

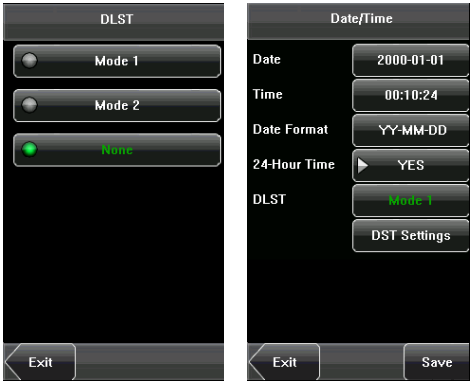
DLST, también llamado como horario de verano, este sistema fue creado en horarios locales como ahorro de energía. Tiempo después este sistema fue unificado y llamado “DLST”. Usualmente el tiempo se adelanta una hora en el verano. Lo que provoca un ahorro de energía y en el tiempo de otoño es recuperada esta hora. Esto ya es un hecho en diferentes países. Al presente cerca de 110 países adoptan el DLST.



Operación:

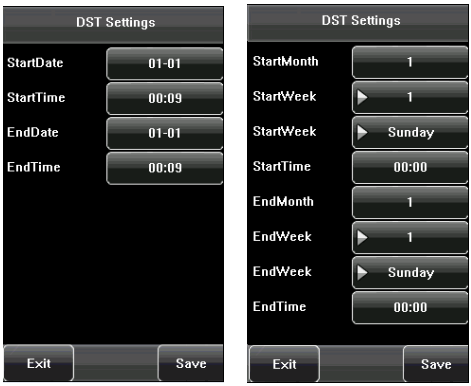
Seleccione el modo DLST primero. Se incluye modo 1, modo 2 y ninguno, por default se encontrara desde la fábrica en ninguno.

1. Clic en [Ninguno] para mostrar el modo seleccionable de DLST.
2. Seleccione el modo DLST y regrese a la interfaz:



3. Clic en [Configurar DST], para entrar a la interfaz de configuración.

Modo1 Modo2



4. Después de Configurar haga clic en [Salvar] para terminar y regresar.

9. Auto Prueba

En el test de auto prueba le permitirá revisar la función de cada uno de los componentes del equipo como el teclado, sonido, comandos de voz y por supuesto realizar una calibración de la pantalla touch.

1. Test de pantalla: Se mostraran automáticamente los efectos de color del equipo TFT mostrara una pantalla a color, después solo blanco y solo negro lo que le ayudara a verificar que la pantalla trabaje correctamente y no existan pixeles o líneas de la pantalla dañadas. Podrá continuar con el test o salir presionando [Exit].

2. Sensor de huella★: El equipo verificara que el sensor trabaje correctamente mostrando la imagen de la Huella actual en dimensión solo deberá colocar la Huella en el sensor al iniciar la prueba y se mostrara en tiempo real para salir de la prueba solo presione [Exit].

3. Prueba de Voz: El equipo automáticamente probará los archivos de voz para verificar que el sonido y la calidad sean los adecuados solo deberá presionar la pantalla para escucharlos.

4. Prueba de Rostro: El equipo realizar la prueba de que la cámara trabaje

correctamente y se encuentre en un posicionamiento perfecto para el registro y verificación,

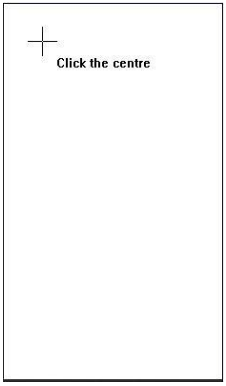
5. Prueba de Teclado★: El equipo se asegurar que cada tecla funcione correctamente. Presione una tecla del teclado en la interfaz para verificar que coincide con el mostrado en la pantalla.

6. Prueba de Tiempo: El sistema revisar el funcionamiento y calibración del reloj realizando una función de cronometro. Solo deberá tocar la pantalla para iniciar y tocarla para parar.

7. Calibración de Pantalla:

Puede realizar la operación del equipo mediante la pantalla touch usando su dedo o una pluma táctil. Si alguna vez el touch pierde sensibilidad podrá realizar la siguiente operación.

Operaciones Para Calibrar la Pantalla:



(1) Presione [Menú] desde el menú de la interfaz principal.

(2) Presione [Calibración] en [Auto prueba] y aparecerá la interfaz para realizar el procedimiento.

(3) Toque el centro de la cruz “+”.

(4) repita el paso 3 siguiendo la cruz “+” en la diferentes posiciones.

(5) Toque le centro de la cruz en 5 posiciones diferentes de manera correcta. Cuando aparezca el mensaje “Calibrando pantalla, espere……” se muestre, la calibración será realizada al final regresara el menú anterior. Si esta falla, lo regresara nuevamente desde el paso 3.

10. Administración de USB

Desde el menú [**Descargar/Cargar**] usted podrá descargar la información de asistencia y almacenarla en una memoria USB y compartirla con el software actualmente usado.

1. Descargar Transacciones: Descargue todas las transacciones de asistencia desde el equipo a la memoria USB.

2. Descargar Usuarios: Descargue la información de usuarios, Huellas e imágenes de desde el equipo a la memoria USB.

3. Descargar Fotos de Usuarios★: Descargue las fotografías de los usuarios desde el equipo a la memoria USB.

4. Cargar Usuarios: Cargue la información de usuarios, Huellas o imagines de rostros desde la USB hacia el equipo.

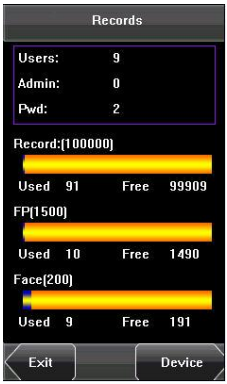
5. Cargar Fotografías de Usuario★: Cargue archivos JPG definidos para ID de usuario desde el USB al equipo para que estas fotos puedan ser mostradas en la verificación del empleado. Vea 12.5 Función Foto ID.

11. Información del Sistema

Podrá verificar el estado de almacenaje y la versión del equipo solo vaya a [Información de sistema]

Registros: Número de usuarios registrados, administradores y contraseñas se mostraran en esta interfaz el total de Capacidad ocupada por las plantillas de Huellas y la Capacidad restante también la Capacidad de transacciones de ocupada será mostrada así como la Capacidad restante.

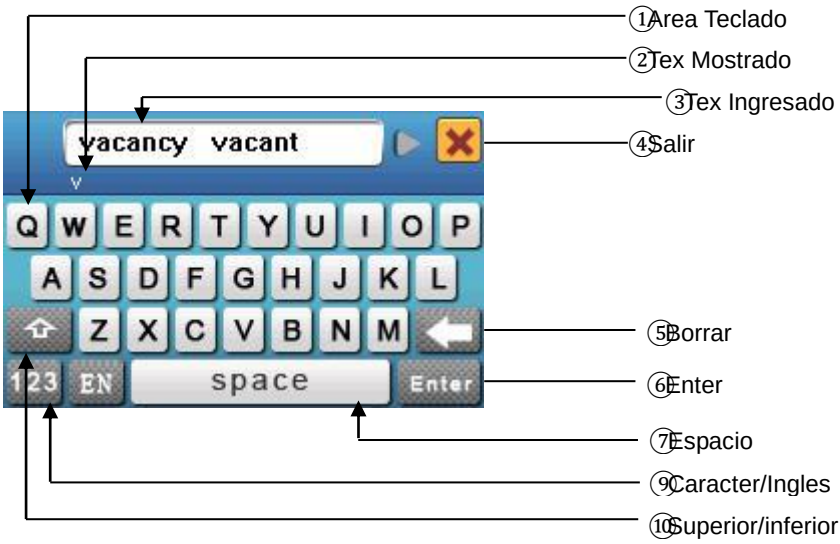
Equipo: Nombre de equipo, número de serie, información de versión, fabricante y fecha de elaboración será mostrado en la opción [**Equipo**].



12. Apéndice

12.1 Instrucciones de Método de entrada T9

El equipo soporta el ingreso de caracteres en inglés, Numero si símbolos. Presione el botón relacionado a la entrada de texto. Por ejemplo presione [Nombre] y se mostrara la entrada de texto:



Para ingresar un nombre realice lo siguiente:

1. Presione [Nombre] en la interfaz [Agregar] como se ve en la figura.

2. ingrese los caracteres de letras y una lista de caracteres relacionados será mostrada.

3. Si el caracter deseado aparece en el área haga clic en este caracter y automáticamente este será el mismo del área de texto ingresado e ingrese el siguiente caracter realizando de Nuevo el paso 2.

4. Al terminar de ingresar el nombre presione [X] para salir del teclado y regresar a la interfaz anterior.

12.2 USB

1. USB Host

El equipo funciona con la opción USB host para enviar datos a un pendrive externo

La transmisión de datos es rápida los equipos tradicionales de Huella solo soportan RS232, RS485 o Ethernet como transmisión como resultado de condiciones limitadas en gran cantidad de datos con el método de USB la transmisión será fácil y rápida ya que este modo es más rápido que cualquier otro, podrá completar el periodo de carga y descarga en tiempos verdaderamente rápidos.

.

2. USB Cliente

Con este modo de comunicación usted podrá tener la conexión entre el equipo y la PC, de esta manera realizar la transferencia de datos e información e incluso realizar el monitoreo en tiempo real del equipo, recuerde que solo algunos equipos cuentan con el modo de conexión de USB cliente en su mayoría esta conexión es solo USB host

.

12.3 Introducción Wiegand★

Wiegand26 es un protocolo de control de acceso establecido por el subcomité estándar de controles de acceso afiliado a la asociación de Seguridad industrial (SIA). Es un protocolo de salida y lector de Proximidad libre de contacto

Wiegand26 define una interfaz entre el lector y el controlador usada en control de acceso, Seguridad y potros campos de la industria. El Wiegand26 ayuda a normalizar el trabajo de los diseñadores y fabricantes de lectores de tarjetas de controlador. Los productos de control de acceso fabricados por nuestra empresa también se han diseñado siguiendo este protocolo.

Señales Digitales

La figura siguiente es un diagrama de secuencia en la que el lector de tarjetas envía señales digitales en formato de bits al controlador de acceso. En este diagrama de secuencia el Wiegand sigue el protocolo estándar de control de acceso de la AIE para el lector de tarjetas Wiegand de 26 bits (un tiempo de pulso oscila entre 20us y 100 ms y el tiempo de salto de pulso oscila entre 200us y 20 ms). Data1 y Data0 son de nivel alto (mayor que Vol.) señales que el lector de tarjetas se prepara para enviar en flujo de datos. El pulso de bajo nivel asíncrono (más pequeño que Vol.) generado por el lector de tarjetas se envía al panel de control de acceso (La onda de diente de sierra como se muestra en la figura a continuación) a través de Datos1 o Data0. Datos1 y DATA0 impulsos no se sobreponen para no generar una forma sincrónica. La siguiente tabla muestra el máximo y el mínimo de ancho del pulso (pulso consecutivo) y el salto del pulso en el tiempo (tiempo entre pulsos) que permite el control de acceso por huella dactilar.

Figura: Diagrama de Secuencia

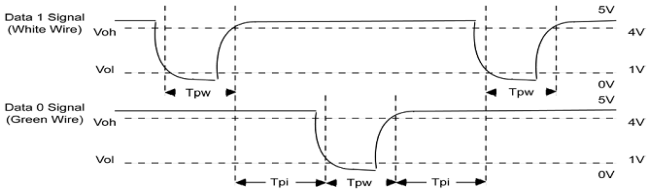


Tabla: Tiempo de Pulso

Símbolo	Definición	Valor típico del lector
Tpw	Ancho del pulso	100 µs
Tpi	Intervalo-pulso	1 ms

12.4 Función de Foto ID★

Esta función es usad apara mostrar la fotografía registrada de un usuario o guardada en una USB y adicionarla a la información de usuario la que aparecerá con su nombre en la verificación exitosa.

[Pasos de operación]

1. Si la foto se toma usando el equipo, esta se mostrar el verificación exitosa al equipo.

2. Para usar una foto guardada en una memoria USB, siga lo siguiente:

1) Cree un folder con el nombre de “foto” en el USB, y guarde las fotos en este folder.

2) La fotos deberán estar en un formato LPG y ser nombradas con ID del usuario. Por ejemplo, para el usuario con el ID -154, el nombre de su fotografía deberá ser 154.jpg.

3) Inserte la USB en la Ranura del equipo y seleccione administración de USB -> Cargar-> Cargar fotos. Después la foto será mostrada en cada verificación de usuario.

Nota:

1) La longitud del nombre de usuario no deberá exceder de 24 caracteres.

2) El tamaño recomendado para una foto de usuario es menor de 64k bits.

3) Al cargar una fotografía de usuario la nueva se sobrescribirá en la existente.

4) Para descargar la fotos de usuarios Seleccione Administración de USB -> descarga -> Descargar fotos de usuarios. Un folder con el nombre de “Foto” Sera automáticamente creado en la USB y todas la fotografías descargadas serán enviadas del equipo directamente a esta carpeta.

12.5 Códigos de Trabajo★

[Descripción de Función]

El concepto de códigos de trabajo es incluido para facilitar a la información de los registros de usuarios en diferentes casos. Por ejemplo, si definimos “1” y para comer, “2” para ir al doctor “3” para fumar y agregamos un valor correspondiente cuando se realice esta opción. De esta manera el software podrá diferenciar fácilmente de vario eventos 1, 2 y 3.

[Descripción de Operación]

Puede configurar "**Código de Trabajo**" seleccionando **Menú → administración de datos.**

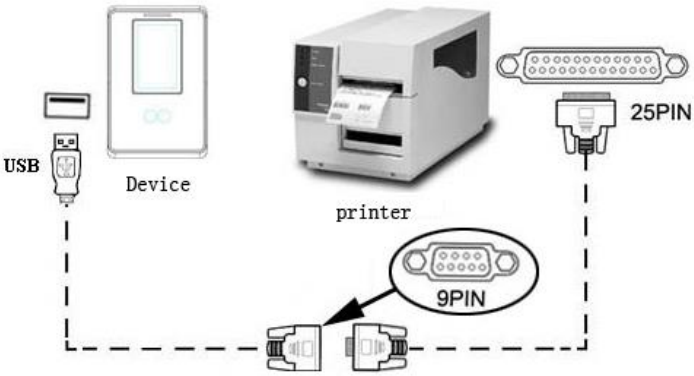
12.6 Función de impresión★

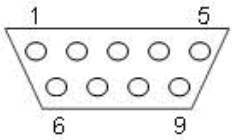
◆ Impresora externa

[**Explicación**]

Los equipos contienen solo una interfaz de exportación USB. Para conectar una impresora serial, primero use el cable USB para convertir a RS232. Después de que la impresora se conecte la función de impresión será habilitada. La salida de Contenido podrá ser vista desde la terminal.

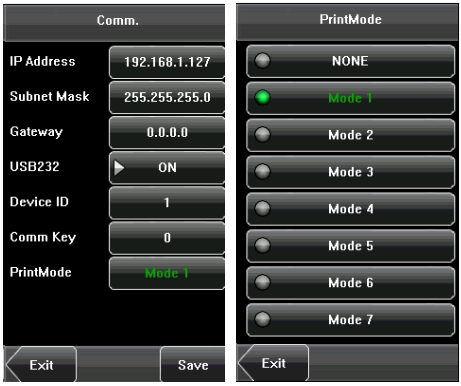
[**Conexión**]



Use el cable USB para convertir a RS232 y conectar por RS232.	Equipo Impresora 2 TXD <-----> 3 RXD 3 RXD <-----> 2 TXD 5 GND <-----> 7 FG
RS232 Orden de línea de PINS	

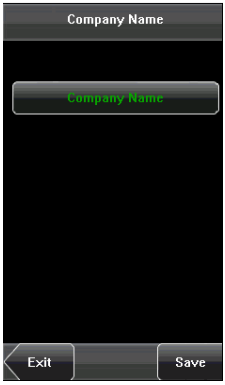
[**Instrucciones**]

En el menú del equipo ingrese **Menú–>Com. –> Com.** Seleccione el modo de impresión. Existen 6 modos a escoger.



Nota:

1. cuando el modo de impresión es el 4, podrá entrar a la interfaz para agregar el nombre de la compañía.



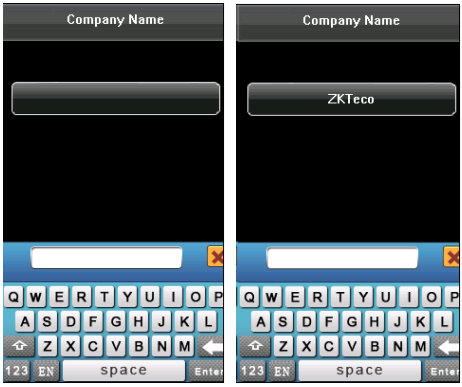
Nombre de Compañía★: Agregue el nombre de la compañía. Y este será impreso a igual que los demás datos del modo de impresión 4.

Operación:

(1) Presione [nombre de compañía], y el teclado que aparecerá escriba el nombre al finalizar solo presione [X].

Para detalles de operación del teclado vea 12.1 T9 Instrucciones de entrada.

(2) Después de ingresar el nombre presione [Salvar] para salvar la información y regresar a la interfaz anterior o presione [Exit] para regresar a la interfaz sin salvar la información.



2. Cuando el modo de impresión es el modo 5, mostrara lo siguiente después de una verificación.

Presione **Si** e imprimirá el registro del modo 5. Presione "NO" para no imprimir.

Por ejemplo: Pedro paso su tarjeta a las 11:02:42 en junio 11, 2012, hay diferente formatos de impresión para seleccionar, como se muestra:

Versión 1

000000001 1 12-06-11 11:02:42 I

Versión 2

ID. NO: 000000001

Date Check-In

12-06-11 11:02:42

Versión 3

1 000000001 San

12-06-11 11:02:42

Versión 4

Control Asistencia

==========

Check-In

11:02…..11/06/2012

ID.NO…. 000000001

======= ¡Gracias! =======

Versión 5

000000001 12-06-11 11:02 Check-In

Versión 6

ID.NO: 000000001

Nombre: Pedro

Check-In

12-06-11 11:02:42

Noticia:

(1) En el modo 2 el papel será cortado automáticamente.

(2) Si desea personalizar otros modos de impresión de acuerdo a sus necedades por favor contacte a su representante o a su oficina local de ZK.

12.7 Modo de Verificación en Multi-Combinación★

Además de que esta función sólo es para equipos de control de acceso de huella digital ha sido agregada a la mayoría de las máquinas sólo tienen dos maneras de verificar por huella digital y contraseña, podemos proporcionar un modo de autenticación multi-combinación personal o de grupo para el área de control de acceso en alta seguridad el tipo de verificación principal incluye cinco elementos que son Número de usuario.

Nota: La tarjetas RF son usadas como modo de tarjeta ID.

A continuación se muestran los símbolos ilustrados y su significado.

- **"/" es o**
- **"+" Siga la siguiente operación**
- **"&" es y**
- **FACE (Rostro)**
- **FP (huella)**
- **PWD (Contraseña)**
- **RF (Tarjeta RF)**
- **PIN (ID de usuario)**

Si la huella, Rostro, Contraseña y tarjeta fueron registrados por el usuario, el proceso será el siguiente.

Tipo	Lo que se hace
FACE&PIN/FP/PW/RF	FACE+PIN o RF o PW o RF serán verificados
	1) PIN++FACE(1:1) 2) FP(1:N) 3) PIN+PW+“OK” 4) RF(1:N)
FP&PW	FP + PW serán verificados
	1) FP(1:N)+PW+“OK” 2) PIN+FP(1:1)+PW+“OK” 3) PIN+PW+“OK”+FP

FP&RF	FP + RF serna verificados
	1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)+RF
FACE&FP	FACE + FP serán verificados
	1) FP(1:N)+FACE 2) FACE(1:N)+FP 3) PIN+FACE(1:1)+FP 4) PIN+FP(1:1)+FACE
FACE&PW	FACE + PW serán verificados
	1) FACE(1:N)+PW+“OK” 2) PIN+FACE(1:1)+PW 3) PIN+PW+FACE
FACE&RF	FACE + RF serán verificados
	1) FACE(1:N)+RF 2) PIN+FACE(1:1)+RF 3) RF(1:N)+FACE
FP	Solo FP se verificara.
	1) PIN+FP(1:1) 2) FP(1:N)
PW	Solo PW se verificara
	PIN+PW+“OK”
RF	Solo RF se verificara
	RF(1:N)
FACE&PIN	FACE + PIN será verificado
	PIN+FACE(1:1)
FP/RF	FP o RF se verificara
	1) PIN+FP(1:1)

	2) RF(1:N) 3) FP(1:N)
PW/RF	FP o RF se verificara
	1) PIN+PW+“OK” 2) RF(1:N)
FP/PW	FP o PW se verificara
	1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+PW+“OK”
PIN&FP	PIN + FP se verificara
	PIN+FP(1:1)
FP&PW&RF	FP + PW + RF se verificara
	1) FP(1:N)+PW+“OK”+RF 2) PIN+FP(1:1)+PW+“OK”+RF 3) RF(1:N)+PW+“OK”+FP 4) PIN+ PW+“OK”+FP(1:1)+RF
PIN&FP& PW	PIN + FP + PW se verificara
	1) PIN+PW+“OK”+FP(1:1) 2) PIN+FP(1:1)+PW+“OK”
FP & RF/PIN	FP + PIN, o FP + RF se verificara
	1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)
FACE&FP&RF	FACE + FP + RF se verificara
	1) FACE(1:N)+FP+RF 2) FP+FACE(1:1)+RF 3) RF(1:N)+FACE+FP 4) PIN+FP(1:1)+FACE+RF

	5) PIN+FACE(1:1)+FP+RF
FACE&FP&PW	FACE + FP + PW se verificara
	1) FACE(1:N) +PW+“OK”+FP 2) FP+PW+“OK”+FACE(1:1) 3) PIN+FP(1:1) +PW+“OK”+FACE 4) PIN+FACE(1:1) +PW+“OK”+FP 5) PIN+PW+“OK”+FP+FACE

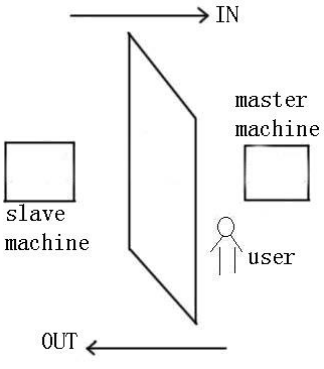
Nota: Para verificaciones combinadas, será mejor registrar los elementos que serán utilizados o la verificación fallara.

12.8 Anti-Pass Back★

[Explicación]

A veces algunas personas siguen a otras por las puertas lo cual brindara inseguridad a nuestro control de acceso. Para evitar estos riesgos esta función puede ser activada. El registro debe coincidir en el registro de salida, o la puerta no se abre.

Para esta función necesita dos máquinas trabajando juntas una se instala en el interior de la puerta (maestro), la otra se instala fuera de la puerta (esclavo). Se adoptara la comunicación entre ambos equipos



mediante wiegand

[Principio de funcionamiento]

La máquina principal debe tener entrada Wiegand y la máquina esclavo Salida Wiegand. Conecte la salida Wiegand de la máquina esclavo a la entrada Wiegand en la máquina master. En la Salida Wiegand de la máquina esclavo no debe poseer ID de máquina.

[Función]

La función del antipassback consiste en asegurarse de que los usuarios completen siempre el ciclo de entrada y salida, esto quiere decir que si el usuario A entra detrás del usuario B pero el usuario A no registro su entrada este mismo al tratar de salir la terminal interna no le brindara la salida al no tener el registro de entrada del usuario A, mediante la conexión wiegand ambas terminales mantienen la comunicación y se transmitirán la información de registros en este caso será la terminal esclavo quien enviara todo registro a la terminal maestro para que esta a su vez se encargue de realizar el proceso de antipassback

[Operación]

1. Seleccione Modelo

Maquina Master/Maestro: La máquina con entrada Wiegand en función a excepción del lector F10 Maquina Esclavo/Slave: La máquina con salida Wiegand en función

2. Configuración del Menú

Anti-pass back

Existen 4 opciones entrada/salida anti-pass back, salida anti-pass back, entrada anti-pass back, and ninguno.

Salida anti-pass back: Sólo un último registro de usuario se encuentra en el expediente la puerta podrá ser abierta.

Entrada anti-pass back: Sólo el último registro del usuario estará fuera de registro la puerta podrá ser abierta.

Estado de equipo: Hay 3 opciones: Control de entrada, control de salida y ninguno.

Control de entrada: Cuando se establece, los registros verificados en el dispositivo son solo reportes de entrada

Control de salida: Cuando se establece, los registros verificados en el dispositivo son solo reportes de salida

Ninguno: Cuando se establezca cierre la función anti-pass back del dispositivo.

3. Modifique el formato de salida Wiegand

Cuando los dos dispositivos se comunican sólo se reciben las señales de Wiegand sin ID de dispositivo. Ingrese al menú-> comunicación opción->Wiegand o en el software -> Configuración básica -> Administración de dispositivos -> Wiegand, a modificar "Formato definido" como “wiegand26 sin ID del dispositivo".

4. Enrolar usuario

El usuario debe estar en la máquina maestro y esclavo al mismo tiempo y el PIN de usuario debe ser el mismo. Por lo tanto es necesario para inscribir un usuario en la máquina maestro y esclavo de la máquina al mismo tiempo.

5. Instrucción de Conexión

La conexión Wiegand deberá ser adoptada como se muestra en la siguiente figura:

:

Master		Slave
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

12.9 Declaración de Derechos Humanos y Privacidad

Estimados clientes:

Gracias por elegir los productos de reconocimiento de venas, Como proveedor de renombre mundial de tecnologías y servicios biométricos prestamos mucha atención al cumplimiento de las leyes relacionadas con los derechos humanos y la privacidad de todos los países en el desempeño de constante investigación y desarrollo.

Por la presente, hacemos las siguientes declaraciones:

1. Todos nuestros dispositivos de reconocimiento de venas de dedo sólo reconocen los puntos característicos de las venas del dedo en lugar de las imágenes de venas del dedo y por lo tanto están involucrados los problemas de privacidad.
2. Los puntos característicos de las venas del dedo recogidos por nuestros productos no se pueden utilizar para restaurar las imágenes de las venas originales y por lo tanto están involucrados los problemas de privacidad.
3. Nosotros como el proveedor del equipo no podremos ser legalmente responsables, directa o indirectamente, por las consecuencias que pudieran derivarse de la utilización de nuestros productos.
4. Por cualquier controversia relacionada con los derechos humanos o la privacidad al usar nuestros productos, póngase en contacto con su empleador directamente.

Nuestros productos de reconocimiento de vena para uso de la policía o las herramientas de desarrollo apoyan la colección de las imágenes de las venas dactilares originales. En cuanto a si un tipo de colección de venas constituye una violación de su privacidad por favor póngase en contacto con el gobierno o el proveedor del equipo final. Nosotros el fabricante del equipo original no podremos ser considerados legalmente responsables de cualquier infracción.

12.10 Respetuoso con el medio ambiente Uso y Descripción

Los Períodos de utilización al Entorno óptimo (EFUP) marcados en este producto se refieren al periodo de seguridad del tiempo en el que el producto sea utilizado bajo las condiciones especificadas sobre las instrucciones del producto sin fugas de sustancias nocivas y perjudiciales.

El EFUP de este producto no cubre las piezas consumibles que deben ser reemplazados en una base regular tales como baterías y así sucesivamente. El EFUP de las baterías es de 5 años.

Nombres y concentración de sustancias o elementos tóxicos y peligrosos

Partes	De sustancias o elementos tóxicos y peligrosos					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	×	○	○	○	○	○
Chip capacitor	×	○	○	○	○	○
Chip inductor	×	○	○	○	○	○
Chip de diodo	×	○	○	○	○	○
ESD componentes	×	○	○	○	○	○
Zumbador	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
tornillos	○	○	○	×	○	○

○: Indica que esta sustancia tóxica o peligrosa contenida en todos los materiales homogéneos para esta parte se encuentra por debajo del requisito límite en SJ/T11363-2006.

×: Indica que esta sustancia tóxica o peligrosa contenida en al menos uno de los materiales homogéneos para esta parte está por encima del requisito de límite en SJ/T11363-2006.

Nota: 80% De las piezas de este producto está fabricadas con materiales respetuosos al medio ambiente no peligrosos. Las sustancias peligrosas o elementos contenidos no pueden ser reemplazados con materiales respetuosos del medio ambiente en la actualidad debido a las limitaciones técnicas o económicas.